Office of Fair Trading

# Internet shopping

An OFT market study

## CONTENTS

# EXECUTIVE SUMMARY

## Key findings

In just a few years, the internet has had a profound impact on UK retailing, enabling businesses to sell and shoppers to buy products from anywhere in the world at any time. Internet shopping is bringing huge benefits to millions of consumers and thousands of businesses.

Our fact-finding study, however, also identified some areas where more could be done to ensure people get the most from buying online, and can feel confident and protected when doing so. Our findings include:

- **Awareness of online shoppers' rights is low for businesses and consumers.** Many businesses are not fully complying with laws to protect shoppers. In part, this reflects a need for higher profile guidance. There are many advisory services, but no single overall dedicated source – especially to help businesses to be aware of all they need to know when selling online.
- **The anonymity, speed of change and borderless nature of the internet, can pose particular challenges for the enforcers of shoppers' rights.** However, new developments in the powers, roles and relationships between enforcers provide an opportunity to bring more co-ordination to how they can overcome these problems. In some areas, the laws that protect online shoppers also need some modernising.
- **Shoppers have significant fears about security and privacy, which put some off buying online altogether.** Internet users who are too worried to buy online could be missing savings of £175m to £350m each year. There are risks from using the internet generally, but it is not apparent that such high levels of fear about shopping online are warranted, provided shoppers and businesses take sensible precautions. However, awareness of these precautions, as well as the remedies available if something goes wrong, remains weak. Advice to shoppers needs to inform without scaring them.
- **By searching more effectively, shoppers can find big savings.** We estimate these could amount to £150m to £240m each year. But they may also be hindered by unexpected additional charges which are sometimes added in the latter stages of a purchase. These charges annoy shoppers, and lead to some paying more than they might. We estimate that shoppers pay £60m to £100m a year in unexpected additional charges.

## Next steps: A strategy for internet shopping

In this exploratory research, we have identified important areas for further work – many of them relating to the need to raise awareness of rights and protections. In developing the right solutions, we want to work more closely now and in the future with organisations that have an interest in ensuring internet shoppers are protected and can feel confident when they buy online. We will encourage industry to self-assess, to make sure it is complying with the relevant legislation. Enforcement may ultimately be considered to target outstanding breaches that create clear detriment.

As well as addressing the issues we identified, we need to look ahead to new developments. The backdrop to internet shopping is changing at a dizzying pace, with developments such as mobile phone commerce, targeted advertising, digital delivery, Web 2.0 and virtual worlds. Furthermore, the law and its enforcement are evolving with the recent implementation of the Consumer Protection Co-operation Regulation ('CPC'), the introduction of the Consumer Protection from Unfair Trading Regulations 2007 ('CPRs'); as well as the establishment of the Local Better Regulation Office (LBRO), and possible future changes from the review of European consumer protection legislation by the European Commission.

We will now therefore:

- Consult key interested parties, to develop closer working relations and remedies to the issues we identify in our report
- Put in place a forward-looking strategy for internet shopping which, in particular, will include:
  - Working closely with Trading Standards Services, to identify how best to enhance and assist future enforcement of online shoppers' rights
  - Developing a strategy of targeted, innovative campaigns to raise awareness of shoppers' rights, as well as other issues such as effective search, risks, redress and protections

We will announce the details of this strategy, and how we will be implementing it, by the end of the year.

## Background

The scale and growth of internet shopping is impressive. In 2005, the most recent year for which reliable figures are available, sales to households were over £21bn – a fourfold increase during the previous three years. It is benefiting millions of people and thousands of businesses. Over 20 million UK adults shopped online in 2005, with 56 per cent of internet shoppers we surveyed having spent over £500 each during the year. In the same year, an estimated 62,000 UK businesses were selling online to households.

We found that people shopped online because they find it convenient, it increases their choice and helps them to hunt for lower prices. Retailers sell online to reach more customers, to sell around the clock and in reaction to competition from rivals.

However, the rapid growth of internet shopping means it is more important than ever that online retailers know their obligations to their customers, and that shoppers can feel confident about addressing any problems. In our fact-finding research, we therefore looked at why people and businesses use, or do not use, the internet to buy and sell products; their experiences; and what happens when things go wrong.

## Our main findings

### Awareness of online shoppers' rights is low

When you buy at a distance from a UK-based business, including online, you have all the rights you would have if you had bought on the High Street plus, for most products, additional rights to encourage confidence in this method of buying.

The Distance Selling Regulations ('DSRs') give buyers:

- A right to know who they are dealing with
- Key information about what they are buying
- An unconditional right to cancel within seven working days, and to receive a full refund
- Protection against online payment card fraud

The Electronic Commerce (EC Directive) Regulations 2002 ('ECRs') also require businesses to, among other things, provide an email address for direct and effective communication.

Shoppers need to know, when they buy, that they have the right to cancel, so that they do not unnecessarily keep products that on examination they do not want. However, we found that more than half (56 per cent) of the internet shoppers we surveyed online did not know about their right to cancel, and many (29 per cent) also did not know where to turn to get advice on their rights.

We also found that a lot of traders had a weak awareness of the law themselves. For example, in our survey of UK-based online traders, 28 per cent said that they were not aware or only slightly aware of the laws applying to internet shopping, and two-thirds (66 per cent) had never sought advice on them. One fifth of online electrical retailers did not think that buyers had a right to cancel, and more than half wrongly thought that they could withhold the cost of outward delivery when refunding shoppers.

When we looked at websites, we found that one in ten (12 per cent) of electrical sites and nearly four in ten (39 per cent) of music retailers' sites selling CDs did not appear to mention the cancellation period. Furthermore, there was evidence that some sites might be trying to impose conditions that could prevent or at least deter consumers from exercising their cancellation rights. For instance, 59 per cent of electrical sites stated at least one condition on consumers' rights to cancel and receive a refund which may have led to a breach of the regulations. Furthermore, more than one fifth of sites we looked at may have been breaching the regulations by not providing an email address.

Businesses told us that guidance on the key legal requirements should be clearer and have a higher profile. While many different sources of advice are currently available, most tend to address separate issues, such as general consumer rights, distance selling obligations, the law on privacy or guidance about online threats and safety. Many organisations said that they would welcome a single clear dedicated source or signpost, to cover all the information needs for internet sellers and shoppers.

We asked internet shoppers if they had experienced any problems when shopping online. Nearly a quarter (23 per cent) told us that they had experienced a problem in one of their online transactions in the previous year, equivalent to an estimated one in 58 purchases. It was difficult accurately to compare their responses with the experience of shopping through other channels, but our data suggest that the volume of consumer complaints does not appear unusual when compared to other distance selling channels, and that the types of complaints match those for mail order.

Shoppers and online traders told us that delivery was where most problems cropped up: indeed it accounted for nearly half (48 per cent) of all the problems people said they had experienced (most typically as late or non-delivery). While we did not explore delivery problems in detail, because they are common to distance selling generally, it is clear that they have important economic implications. The annual economic detriment from unresolved delivery problems for online sales could be as much as £25 million to £55 million per year, excluding time and effort spent on resolving problems.

Better communication between the main parties involved in delivery could be key to addressing some of the problems experienced. Businesses told us of measures being put in place to meet the rapidly increasing demand for delivery services resulting from the growth of internet shopping.

## Next steps

We will develop and implement a strategy employing the most effective and innovative ways actively to raise business and consumer awareness of online shoppers' rights – both directly and by working with third parties. We will also look into whether and how the wider range of relevant advice to internet traders and buyers could be more co-ordinated. This will include raising awareness of how to prevent the most typical problems, like difficulties with delivery.

It will also include raising awareness of what to look for to identify the location of a trader and how to handle problems that arise when buying from abroad.

We will encourage industry to self-assess, to make sure it is complying with the relevant legislation. Enforcement may ultimately be considered to target outstanding breaches that create clear detriment.

## The laws protecting online shoppers

The regulations giving online shoppers additional rights derive from European Directives. These laws appear broadly fit for purpose at present. We did, however, identify a number of areas where they may need to be revised to take account of how internet shopping is evolving. We have brought these to the attention of the European Commission, who are currently reviewing how they might need to be improved.

We also looked at the role of the key regulations as they relate to 'online auctions'. These rapidly growing electronic marketplaces are a valuable development, with millions of successful transactions every year, accounting for spend using payment cards of £2.8 billion in 2005. But we found that about half (52 per cent) of the online survey respondents who had bought items from an auction site in the last 12 months had experienced at least one problem in the past year. Most of these problems mirrored those of internet shopping generally, although some buyers perceived that they had been victims of deceptions (such as counterfeiting, or sellers bidding up their items). While the value of the items involved was typically low and a high proportion chose not to complain, of those that did complain, four in ten (39 per cent) had given up trying to resolve the problem.

A range of regulations potentially protect users of online auctions, but consumers face a number of uncertainties when buying on them. In particular:

- Generally, users of online auctions are protected in much the same way as other online purchasers. There is some uncertainty as to whether the DSRs apply, although the ongoing EC Review may help to resolve this.
- We found that 60 per cent of online survey respondents who bought items from an online auction wanted to know whether they were buying from a business. This affects both their confidence and their rights. However, it is not always clear whether sellers are trading as a business, and buyers tend to use a range of indicators to try to judge it (some of them less reliable than others). At the margins, even sellers may not know if they are operating as a business.
- There are also examples where there can be no doubt that products are being sold in the course of a business. While business sellers are required by the regulations to provide their name and address, this does not always happen.
- Auction platforms are typically not liable to consumers for problems with products or sellers. They do not have liability for unlawful activity, such as sales of illegal goods, unless they have actual knowledge of illegality. Given this, consumers need to be aware of the risks involved in buying on such sites and to take sensible precautions.

## Next steps

We want to work with the online auction sites and others to ensure that businesses selling on such platforms know how to comply with their legal obligations to consumers. Our strategy to improve consumer and business awareness will include advice in this area, as well as how to deal with deceptive practices. We also want to investigate further how well the online auction sites are addressing issues like counterfeiting and consumer concerns about the potential for bid manipulation.

## The internet brings challenges for enforcers

Our research suggested that enforcement officers face particular challenges in addressing online shopping – especially in tracing rogue traders. Traders can sell from any location in the UK or abroad and quickly set up or shut down operations. The rapid pace of technological change, coupled with the range of parties that may have an involvement in a transaction can also make it a potentially complex environment in which to conduct investigations.

There are already good examples of enforcement agencies and advisory bodies providing advice to businesses and consumers about online shoppers' rights. We also found some promising examples of proactive work, for instance to assess compliance; to liaise with the internet industry to obtain information on traders; and to co-ordinate activities with other enforcers to achieve successful outcomes. However, despite these efforts, awareness of and compliance with consumer protection laws specific to distance selling could be better. We see potential for greater co-operation between enforcers to ensure greater consistency in how enforcers assess and deal with problems related to internet traders. Good practice should be spread across the whole country.

There is currently no national risk-based approach to identifying problems and aligning the most appropriate response. This needs to be considered within the broader context of other current initiatives which form part of the government's better regulation agenda that will have an impact on local enforcement in general. This includes the establishment of the Local Better Regulation Office (LBRO) with its aim to improve the effectiveness and consistency of local authority regulatory services.

We also considered the enforcement implications of international internet trade. Online cross-border trade is not as substantial as some might think – accounting for seven per cent of the online sales of the UK businesses we surveyed, and less than one-tenth of UK shoppers' online spend. Furthermore, most cross-border internet purchases are from European countries, and the buyers are therefore covered by a common framework of protections.

However, outside Europe, the protections for consumers are less well established. Some international agreements and networks exist, although these have tended to address general threats to internet users, such as spam and scams. For instance OFT's ScamBusters Group has been working closely with international enforcement partners to combat mass marketing scams. These partnerships could provide a valuable basis on which to focus more attention on protecting consumers' rights when buying from online traders abroad.

## Next steps

We invite the views of enforcement partners and will explore with them how to enhance enforcement for online shopping in the future. In line with the principles of a targeted, risk-based approach, currently being established for enforcers, an issue for further consideration could be how best enforcers can target their activity according to the greatest risks and potential detriment for online consumers. Other solutions to consider could include:

- working with industry players who may be able to help with tracing website owners
- investigating possible new tools and techniques, and pooling skills and knowledge in centres of expertise for enforcement staff to call upon
- greater central support in identifying national patterns in complaints
- better active monitoring and surveillance approaches, such as those adopted in some other countries
- greater communication and co-ordination between the key agencies
- improved international co-operation in addressing problems arising from cross-border shopping

## Shoppers have significant fears about security and privacy

Although internet sales have been increasing for years, this does not necessarily mean that they are growing as much as they might. The latest reliable figures, from 2005, suggest that online sales were still only three per cent of all retail sales, and only six per cent of businesses were selling online to households. We found that there are many reasons why businesses and shoppers might not want to use the internet to buy and sell, including lack of internet access, products not being appropriate, or simply no desire to use it. However, some were being deterred by concerns about using the internet to buy, and although many people were willing to shop online, most had fears about doing so. Confidence and trust are important to the success of internet shopping. Forty-two per cent of businesses not selling online told us that increased consumer confidence would make them more likely to.

Futhermore, 79 per cent of internet users we surveyed were very concerned about the risks to the security of their payment details from online shopping. Indeed we estimate that 3.4 million people were prepared to use the internet, but not willing to shop online because of a lack of trust or fears about personal security. Their missed savings could amount to between £175 million and £350 million each year. Although online shoppers seem to gain confidence over time, even experienced ones remained worried about their financial security and privacy.

People told us that their fears stemmed from stories in the media or spread by word of mouth, their receipt of spam and phishing emails, as well as advisory campaigns and advertising. The organisations we spoke to told us that the public's fears about internet shopping were understandable, given the relatively unfamiliar and fast evolving nature of the internet, and were likely to be influenced by regular stories about new threats. However, many also thought that shoppers' worries about buying online were excessively high.

There is a lack of reliable data on the prevalence and significance of the risks from internet shopping itself. However, some of the dangers commonly associated with internet shopping may be more a result of data lost offline or through general internet usage, rather than the result of having shopped online.

Nevertheless, there are risks attached to using the internet, and to selling and shopping online, which need to be taken seriously. To guard against risks to their businesses and to address consumers' concerns (which put some off shopping online altogether), it is in traders' best interests to consider the range of technical and other protective measures they can take.

Likewise, online shoppers can reduce risks by taking precautions and watching for warning signs. Provided they do so, it seems unlikely, at the time of writing, that they will be at substantially more risk than if they use other means of buying at a distance. Even if online shoppers experience the fraudulent use of their payment card details, they have regulatory protections which mean that they are unlikely to have to pay anything.

However, public awareness of these precautions and protections remains weak, despite campaigns and numerous sources of advice. One in five (19 per cent) internet users we surveyed never checked the security of a site and 34 per cent only do sometimes. Many people also do not recognise that they need to take some responsibility for their protection online, believing that this is solely the role of businesses and other organisations.

Awareness campaigns, as well as commercial advertising may also be scaring people away from shopping online as much as they are informing them. Some level of concern may helpfully encourage people to be vigilant, but campaigns need to be balanced, so that shoppers know how to protect themselves, without having excessive fears about online shopping.

### Next steps

We want to work with interested parties in this field to encourage the development and provision of more accurate ways of assessing the risks when shopping online. We also want to work with them to ensure that shoppers have an accurate view of the risks and know how to protect themselves, and that businesses are encouraged to provide a safe shopping environment.
We want to raise awareness of what shoppers can do if something goes wrong. We would like to address, within future work on this, consumers' rights not to receive unwanted emails or to have their information shared without their permission.

## Shoppers need to search effectively

The internet has enabled businesses to establish a new means of selling by setting up their own websites, and adopting new business models to widen their reach. However, the vast range of retailers and offers available to shoppers can make it hard for them to locate and differentiate between competitors. We identified some large differences in prices being charged for similar goods online – for instance, by an average of 30 to 60 per cent of the lowest price for the music and electrical items we looked at. Fortunately, provided they are used well, tools such as search engines and price comparators can help consumers to make informed choices and save money.

However, we found that some consumers could benefit from searching more effectively online, particularly given limits to the numbers and range of traders listed by some price comparison sites. For instance, if a shopper used only one of ten price comparison sites we looked at, they had a 50 per cent chance of finding one of the lowest prices. We estimate that online shoppers who misunderstand how search tools work and therefore limit their search, could miss out on potential savings of £150 million to £240 million per year.

We also found that shoppers often experienced charges added to the initial price. For instance, for 47 per cent of the flights we looked at, the final 'check-out' price was higher than the initial price. For these, the median price increase was 19 per cent, but many increases were much more. For online sales as a whole, we estimate that 1.2 million internet shoppers were unaware of these charges during the buying process, but still went on with their purchase and paid £60 million to £100 million each year as a result.

## Next steps

It is important that consumers appreciate the limitations of search sites and use them as effectively as possible. We will develop ways to raise awareness of how shoppers can make best use of the tools available to them.

There could also be scope to improve the quality of information provided to consumers by extending advertising self-regulation to websites. We will explore with the Committee of Advertising Practice whether their remit could be extended to cover websites.

# 1 INTRODUCTION

1.1. In a little more than a decade, the internet has revolutionised the lives of millions of its users. Our study explores one aspect of this revolution: its growing use by businesses and individuals as a retail channel.

1.2. In 1995, someone wanting to buy an old Betamax video recorder could spend weeks scouring specialist shops and markets, placing adverts in collectors' magazines or calling individual dealers. If they wanted to buy a flight, they could visit or call their local travel agents and wait to receive the tickets in the post or collect them in person. If they wanted to buy a former hit song, they could travel to the nearest record shops and hunt for it, or order it and pick it up some time later. They could then drive to a local car boot sale, to trawl through the items on offer from other individuals, before driving home with some bargains.

1.3. A decade later, without moving from their seat, the same person might find and buy the video recorder in minutes, possibly in another country. Within the same hour they could have compared flight prices and times from many providers, bought and already received their 'electronic tickets'. They could then click on a music download site and be listening to their favourite song in the same time that it would have taken to get ready to go to the shops. Finally, they might take delivery of the bargain they bought at an online auction and leave some comments on the site, to let other shoppers know whether they were satisfied with the transaction.

1.4. The scale and growth of internet shopping is impressive. In 2005, sales over the internet by UK non-financial businesses to households were over £21bn – a fourfold increase in only three years.[1] But it also raises new questions about risks and shoppers' confidence when buying at a distance, as well as the relevance and effectiveness of the laws protecting them, many of them developed before the recent growth in internet shopping. As a public authority, whose role is to make markets work well for consumers, the Office of Fair Trading needs to consider these issues. This report helps to meet that need.

## Market studies

1.5. We launched this fact-finding market study on 29 April 2006, under section 5 of the Enterprise Act 2002. Market studies[2] are a tool to help identify and address all aspects of market failure, from competition issues to consumer detriment and the effect of government regulations. Although many of our studies explore specific economic markets, they can also review practices across a range of goods and services, as well as the channels through which these products are sold.

1.6. Our studies also vary in their focus and purpose. Some assess well-established concerns, to identify whether and how an apparent problem might be resolved while others, such as this one, seek to explore issues to establish a greater knowledge base for future policy.

[1] Office for National Statistics (2006a) (note figure is for businesses with 10 or more employees).

[2] Guidance on OFT Market Studies can be found at: www.oft.gov.uk/shared_oft/business_leaflets/enterprise_act/oft519.pdf

## Why we conducted the study

1.7. This study reports the findings of our fact-finding research, which identified and explored a broad range of issues raised by the growth of domestic and cross-border internet shopping.

1.8. The growing importance of the internet to the economy and retailing is, in itself, a key reason why we chose to undertake the study: to review whether internet shopping introduces new issues which we should be considering in our role. Furthermore, as a sales channel, the internet is very dynamic with new technology and business models emerging and evolving all the time (for instance, the growth of mobile commerce),[3] with potentially important implications for the protection of shoppers.

1.9. The regulatory framework is also fast changing, with new developments such as the Consumer Protection from Unfair Trading Regulations ('CPRs'), which from 2008 could have important implications for buyer protection online as well as offline. It was also timely for us to look at internet shopping, because our work coincided with the review by the European Commission of eight Directives for protecting consumers (known as the 'consumer acquis'), one of which is the Distance Selling Directive.[4] Our study has already helped to inform the UK's position (see Chapter 6).

1.10. Finally, although we did not start this research with specific concerns in mind, we had identified some particular issues that we felt warranted exploration. In particular, we set out to consider public confidence in the internet as a retail channel, as well as whether the current protections for shoppers meet whatever new challenges might be raised by the development of internet shopping. This report therefore addresses:

- **Attitudes:** how confident are individuals and businesses in the internet as a retail channel, and why? What impacts do attitudes and confidence have on internet retailing?
- **Behaviour:** how and why do consumers and businesses use the internet to buy and sell goods?
- **Experiences:** what do individuals and businesses experience when buying and selling online? What problems do they encounter and how well can they resolve these?
- **Rights awareness:** how well do shoppers know their rights, and businesses know their obligations, when using the internet as a retail channel?
- **Regulations:** to what extent are the current regulations fit for purpose now, and looking to the future?
- **Enforcement:** how well can the current enforcement regime cope with any new challenges raised by internet shopping?
- **Self-regulation:** what role can initiatives such as codes of practice play in raising confidence and providing protection?

1.11. Because the potential range and scale of issues raised by internet shopping is vast and fast moving, we necessarily restricted our focus to some key aspects. Therefore, while this report covers many issues, it is not a comprehensive review of every conceivable issue that may be raised by the growth of internet shopping.

[3] Mobile commerce is the ability to conduct commerce through mobile devices such as mobile phones. A glossary of key terms used in this report can be found at Annexe A.

[4] The European Commission published a Green Paper in February 2007 setting out various options for reform of the eight directives. This requested comments on suggestions for creating an improved framework for consumer protection and simplifying consumers' rights and responsibilities when they shop across the European Union.

## The study's remit

1.12. Much attention is increasingly paid to addressing the impact of fraud, scams and spam on the internet in general. While we consider the impact of these issues on confidence, our main focus in this report is on Business to Consumer (B2C) internet shopping. We explore why consumers and businesses use, or do not use, the internet to buy and sell products; their experiences of using the internet as a retail channel; and what happens when things go wrong.

1.13. Our definition of internet shopping[5] covered transactions by consumers with businesses that enabled them to order online (whether or not the subsequent payment or delivery took place online).[6] We concentrated on legally-sold goods and services ordered online by UK shoppers from UK and non-UK businesses, over the internet.

1.14. We did not explore in any detail:

- Business to Business (B2B) transactions
- Issues that relate to distance selling generally, such as the nature of the provision and market for delivery services
- The infrastructure of the internet (such as cabling) or the supply of access to the internet
- The management of the internet itself (such as the oversight of communications interoperability and address systems), or the regulation of network operators / Internet Service Providers (ISPs)
- People's ease of access to the internet generally (such as social exclusion and the 'digital divide'), and ease of use issues (such as accessibility for users with partial vision, etc)
- Criminal activities on the internet (such as sale of illegal material)[7]
- Ethical issues raised by the selling of certain items (such as animals)
- Internet activity involving no direct B2C purchase of goods or services, such as public services (for instance e-government); 'web communities' such as MySpace or YouTube; user activities such as blogs, podcasts; and free information provision (such as news sites)

1.15. We excluded products or issues where other regulators typically lead (such as utilities, financial products, food standards, communications, broadcasting). We also excluded the provision of auxiliary services, such as consumer credit.

1.16. In the time available, we focused on consumer protection issues while remaining aware that competition can be a factor in these issues. We did not investigate the role or activities of particular companies, or assess competition within specific retail markets. An assessment we commissioned in 2006, of the economic literature on internet shopping did not identify significant new competition concerns arising that could not be addressed under the Competition Act 1998.[8] However, the report did identify the growing importance of new phenomena prompted by the internet, such as search intermediaries and online auctions, which are developments our study has explored.

[5] Throughout this report, we use the terms 'internet shopping' and 'online shopping' interchangeably.

[6] This is similar to the definition used by the Office for National Statistics for e-commerce: 'it is the method by which the order is placed which determines whether a transaction is e-commerce – not the payment or delivery channels' Office for National Statistics (2005a). This in turn is based on a definition adopted by the OECD. See: OECD (2001).

[7] There is some discussion of the online sale of counterfeit products in Chapters 8 and 10.

[8] Internet Shopping – a Review of the Economic Literature – Europe Economics, OFT Paper (2007). At Annexe F.

## Methodology

1.17. In carrying out this study we conducted wide ranging research into internet shopping. A detailed account of our methodology is in Annexe B. Material from our research can be found in the annexes to this report, and include:

- Evidence reviews of the literature in the fields of economics, social research and psychology
- An omnibus survey of 1,000 members of the public
- A telephone survey of over 1,000 individuals to explore our key themes
- An online survey of 1,250 internet users to address some more detailed aspects of internet shopping
- Four focus groups in different parts of the UK with shoppers from a variety of backgrounds, to explore key themes
- A telephone survey of over 1,000 businesses across the UK
- In-depth interviews with 10 businesses of varying size, location and experience
- An in-depth review of the contents of 250 websites
- A review of media content over a four month period
- A survey of enforcement officers in Local Authority Trading Standards Services (TSS)
- Interviews with a selection of TSS officers and OFT Case Officers
- A review of selected enforcement case studies
- A workshop with enforcers
- A consultation of international regulators, via the International Consumer Protection and Enforcement Network (ICPEN)
- Discussions with experts in other countries about their domestic and cross-border experiences

1.18. We also benefited from contributions to an initial small-scale questionnaire survey of key stakeholders, and subsequent discussions with and inputs from over 120 organisations, including:

- Consumer groups
- Relevant trade associations
- Central government departments
- Regulatory bodies
- Businesses in our case study sectors of online auctions, electricals, music and travel

1.19. A list of consulted parties is included in Annexe B. We are very grateful for the time they gave us and their contributions.

## Case studies

1.20. Rather than address every type of market trading over the internet, we selected some case study examples of how the internet is being used to sell specific products. We used these case studies to target our research and to draw wider, transferable lessons for the rest of internet shopping. Findings for these sectors therefore appear throughout this report, which is not a study of each sector in its own right. While they also raised some issues of their own, which we highlight in this report, our focus was on the nature of the online transactions for the products in these sectors.

1.21. We used three product sectors for our case studies:

- **Domestic electrical goods**
- **Travel** (specifically airline tickets with or without accommodation)
- **Music** (hardcopy sales, such as online sales of CDs, as well as downloads)

1.22. We chose these because together they account for a large proportion of online trade. We estimate that, in 2005, around one quarter of online sales to households were of electrical items, flights, music and videos.[9] They also represent a range of different types of goods and services.

1.23. To these three case studies, we added a fourth – **online auctions**. These electronic marketplaces raised issues of their own, which we address separately in Chapter 10.[10]

## Report structure

1.24. The report starts by describing the growth of internet shopping, before reviewing the evidence on shoppers' and businesses' attitudes, behaviour and experiences. Although this was principally a fact-finding study, we identify some areas where action may be needed and suggest some next steps.

- **Chapter 2** provides a factual background to the main findings in the report and explains how internet shopping has grown
- **Chapter 3** examines the drivers and barriers to online shopping, focusing on the extent to which businesses and individuals are confident in using the channel
- **Chapter 4** examines concerns about security and privacy risks, the protections available and levels of awareness of these protections
- **Chapter 5** explores the nature of the problems people typically experience when shopping online and how they react
- **Chapter 6** outlines the domestic consumer protection legal framework and the extent to which consumers and businesses are aware of it
- **Chapter 7** describes the role played by codes of practice in raising confidence and providing protection

[9] OFT estimate using figures from Office for National Statistics (2006a) and Verdict (2007a). Note that music and video sales could not be separated.

[10] We restricted our consideration to issues raised by the nature of these online marketplaces, rather than any specific issues that might be raised by the sale of particular types of products on them (such as tickets for entertainment events).

- **Chapter 8** considers the role and activities of enforcers of rights for online shoppers
- **Chapter 9** considers how businesses seek to attract custom and shoppers search for retailers and products, as well as whether they can make informed choices
- **Chapter 10** addresses some of the issues raised by the growth of online auctions
- **Chapter 11** explores some of the issues raised by cross-border trade
- **Chapter 12** reviews some of the anticipated developments for internet shopping as well as some visions of the future

# 2 THE DEVELOPMENT OF INTERNET SHOPPING

## Summary

The internet is a network of linked computers enabling millions of people to communicate and search for information, as well as to sell and buy products. In the UK, internet access and usage has grown rapidly in the last decade, driven in part by growing access to computers and the take up of broadband.

Internet shopping has grown at a similar rate, with sales worth more than £21bn in 2005. As a retail channel, the internet enables businesses to reach many more customers and to sell around the clock, while shoppers can research and choose products and sellers at any time from any location. The internet has also enabled the development of new business models and the opportunity to trade more easily through third parties.

## Introduction

2.1. This Chapter sets out how internet shopping has grown to date in the UK, and briefly describes the key sectors. It examines how internet shopping differs from other retail channels and what this means for UK businesses and consumers. Finally, it outlines the need to protect those who shop online and introduces some of the key regulatory protections.

## The growth of the internet

### What is the internet?

2.2. The internet is a global 'network of networks', allowing computers around the world to communicate with each other. This network has been in existence since the late 1960s. In the early 1990s a new language for accessing information on this network was created: Hypertext Markup Language (HTML). This allowed the creation of web pages as we now know them.

2.3. A crucial feature of these pages is the ability to move from one to another very simply, by clicking on a hyperlink. This allows for easy navigation between web pages, which are linked together to collectively make up the World Wide Web. The ease of access which this enabled facilitated the rapid expansion of the internet, and its development from a military and research tool into a form of mass communication and commerce. It is hard accurately to measure the true scale of the web, but one estimate in February 2007 suggested it comprised nearly 30 billion pages, on 109 million distinct websites.[11]

2.4. Each computer on the internet has an IP address (for example, 123.4.5.678), a numerical equivalent to a telephone number.[12] Since IP numbers are hard to remember, the addressing system has a second element, the domain name system (DNS), which uses names such as 'www.oft.gov.uk'. One or more domain names can be associated with a particular IP address. The association of IP addresses and domain names allows a user to easily access a website in its physical location on a computer, on a network.

[11] See 'How many web sites are there?' Netcraft (2007).

[12] However, every computer does not necessarily have its own unique IP address, because providers may assign a computer an IP address each time it is connected to the internet.

2.5. The network is operated by Internet Service Providers (ISPs), who have arrangements to exchange communications between one another. The domain name system is managed by international, regional and national bodies. In the UK, Nominet is responsible for registering '.uk' domain names.

## The growth in internet use

### Individuals' use of the internet

2.6. The rapid rise of the internet has been driven to a great extent by dramatic changes in the ability of individuals to access it from home, as well as work and other locations. Computer ownership in UK households has increased considerably over the past five years. By 2005/06, 65 per cent of UK households had a computer, compared with only 33 per cent in 1998/1999. Users' ability to access the internet has increased even more rapidly: by 2005/06, 55 per cent of UK households could access the internet at home, compared with only 10 per cent in 1998/99.[13]

2.7. Another key factor in the last few years has been the ability to connect from home to the internet quickly and easily, as a result of significant growth in broadband availability. By 2006, 40 per cent of GB households had access to broadband – up from 28 per cent just the year before.[14]

2.8. Between January and April 2006, 62 per cent of UK adults reported having used the internet in the previous 12 months, compared with only 40 per cent in October 2000.[15] In February 2007, the UK had the highest proportion of internet users in Europe.[16] Indeed, the internet has become a part of everyday life for many people. A 2006 OFCOM report found that UK adults used the internet for an average of nearly ten hours a week, with access split broadly as two-thirds from home and one third from elsewhere.[17]

2.9. From interviews undertaken between January and April 2006, the two most common reasons why people access the internet are to find out information and to use email, with over eight in ten current UK internet users having done each of these in the previous three months (84 per cent and 80 per cent, respectively).[18] However, shopping has also quickly become another important internet activity: 44 per cent of all UK adults have shopped online.[19]

[13] Office for National Statistics (2006b).

[14] Office for National Statistics (2001-2006). This survey was not expanded to include Northern Ireland until 2006. The figure for broadband access for the UK in 2006 was also 40 per cent.

[15] Office for National Statistics (2001-2006).

[16] On a comparative basis, in February 2007, the UK had 37.6 million internet users (62 per cent of its entire population), compared to 61 per cent in Germany, 50 per cent in France and 70 per cent in the US. The world average was 17 per cent, or 1.1 billion internet users. Source: Internet World (2007).

[17] OFCOM (2006).

[18] Office for National Statistics (2006c). A current internet user is an adult who has used the internet in the three months prior to interview.

[19] OFT estimates based upon Office for National Statistics (2006c).

### Business use of the internet[20]

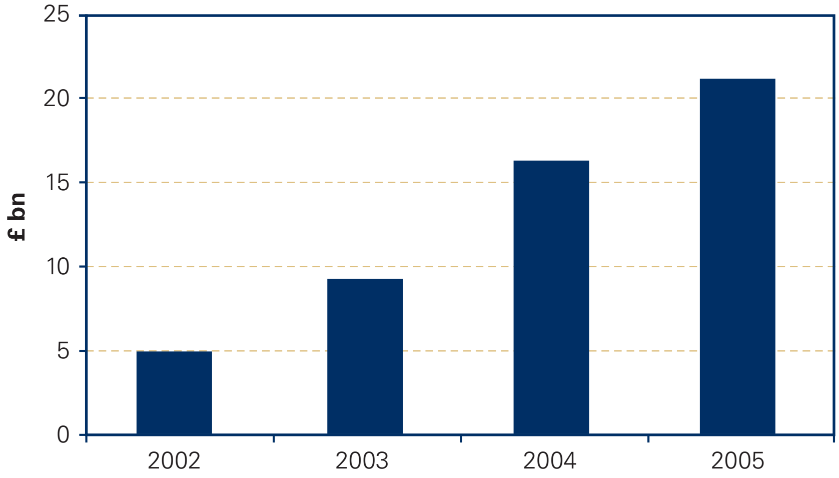
2.10. Businesses have also increasingly been using the internet in recent years. In 2005, 93 per cent of UK businesses with more than ten employees had computers and 89 per cent had internet access. Furthermore, by 2005, 70 per cent of businesses had a website.

2.11. However, although business websites are now commonplace, most businesses simply use them for promotion and communication, rather than to sell through them (in terms of enabling online ordering). In 2005, just 14 per cent (equivalent to 146,000) of UK non-financial sector businesses were believed to sell online to other businesses or to households. Furthermore, only six per cent of businesses (an estimated 62,000) were selling online to households alone. These businesses' sales are the focus of our study.

## How internet shopping has grown in the UK

2.12. The recent growth of internet shopping has been impressive. In 2005, the value of internet sales by businesses to households was £21.4bn – an increase of 30 per cent on the previous year, and more than four times higher than sales of £5.0bn in 2002 (see Chart 2.1).[21] Also in 2005, internet shopping sales accounted for almost three per cent of total UK household spending, compared with less than one per cent in 2002,[22] again nearly a fourfold increase. The Association for Payment Clearing Services (APACS) estimated the number of online transactions in 2005 at 372 million.[23]

**Chart 2.1: Value of internet sales by UK non-financial businesses to households**



Source: Office for National Statistics (2006a)

Base: All UK non-financial businesses (for businesses with ten or more employees)

[20] The estimates in this section are based on Office for National Statistics (2006a). These estimates are for UK non-financial sector businesses only. They should also be treated with caution, because they assume that the rate of businesses with 0-9 employees selling online changed at the same rate as that for businesses with 10 or more employees.

[21] There are many estimates available of the size of internet shopping. For instance, estimates of sales for 2005 included £21.4bn (Office for National Statistics (2006a)), £19.2bn (IMRG) and £8.2bn (Verdict (2007a)). Some measure sales that businesses make to households, while others measure the amount consumers report spending on the internet. The definitions used to define internet sales also differ between sources, with some covering just retail goods, and others including purchases such as air tickets. In our report we mainly use official ONS data, but we also use some detailed data from Verdict to estimate sales in sectors of interest, which are not available from the ONS.

[22] OFT estimates based on data from Office for National Statistics (2006a) and ONS Blue Book 2006.

[23] APACS: www.apacs.org.uk/media_centre/press/06_07_11.html.

## How does the UK compare?

2.13. There are many difficulties in accurately comparing B2C internet shopping internationally, because of variations in definitions, as well as data recording and reporting methods. As a result, the findings of private comparative international surveys often do not tally with domestic data. We agree with the OECD's view[24] that greater standardisation in the recording of data on domestic and cross-border internet trade would be helpful.

2.14. However, what comparative data are available indicate that the UK is a leader in Europe for internet shopping. In 2005, across Europe, in terms of online sales of goods alone (excluding services),[25] the UK was:

- First for size in absolute terms of online retail market at £7.28 billion, ahead of Germany at £6.07 billion
- First in terms of the value of online sales as a percentage of all retail sales, at 3.26 per cent, ahead of Germany at 2.73 per cent
- First in terms of the value of online retail sales per capita at £121, ahead of Belgium at £84.

2.15. In 2006, the European Commission[26] reported that 41 per cent of UK respondents had bought via the internet from UK businesses in the year to March 2006 – compared to an average of 23 per cent across the EU25 and behind only Denmark (46 per cent), the Netherlands (46 per cent) and Sweden (45 per cent).

2.16. Varying survey methods make anything beyond indicative comparisons outside Europe even more difficult. However, what data exist suggest that the UK has a similar record to other leading economies. For instance, the US Census Bureau estimated that online retail sales in the US reached three per cent of total retail sales in the fourth quarter of 2006, an increase from 1.5 per cent in 2002.[27] In Japan in 2004, B2C internet sales were 2.1 per cent of total B2C sales, this percentage having more than doubled since 2002.[28]

## Internet shoppers in the UK

2.17. Internet shopping is still a relatively new phenomenon: we found that 38 per cent of online shoppers had been doing so for two years or less; and 70 per cent had been shopping online for four years or less. Despite this, as we noted above, 44 per cent of UK adults (over 20 million people)[29] have ever purchased something over the internet. This underlines just how big a change there has been in consumers' habits in a short space of time.

2.18. There is striking diversity in online shoppers. Other research[30] has shown that, as might be expected, online shoppers are concentrated in the 25 to 44 age range (accounting for 44 per cent of all internet shoppers). This research also shows that, although their penetration remains low in relation to other age groups, the over-55s are displaying a growing tendency to shop online. The number of shoppers in this age group more than doubled in the years 2004 to 2006, from 1.4 million to 3.4 million.[31]

[24] See OECD (2005a) and OECD (2005b).

[25] Source: Mintel, Home Shopping – Europe, April 2007. Values converted from Euros to Sterling at 2005 exchange rate of €1=£0.68203.

[26] European Commission (2006).

[27] US Census Bureau (2006).

[28] Japan Ministry of Economy (2005).

[29] Estimated by using ONS 2005 mid-year population estimate.

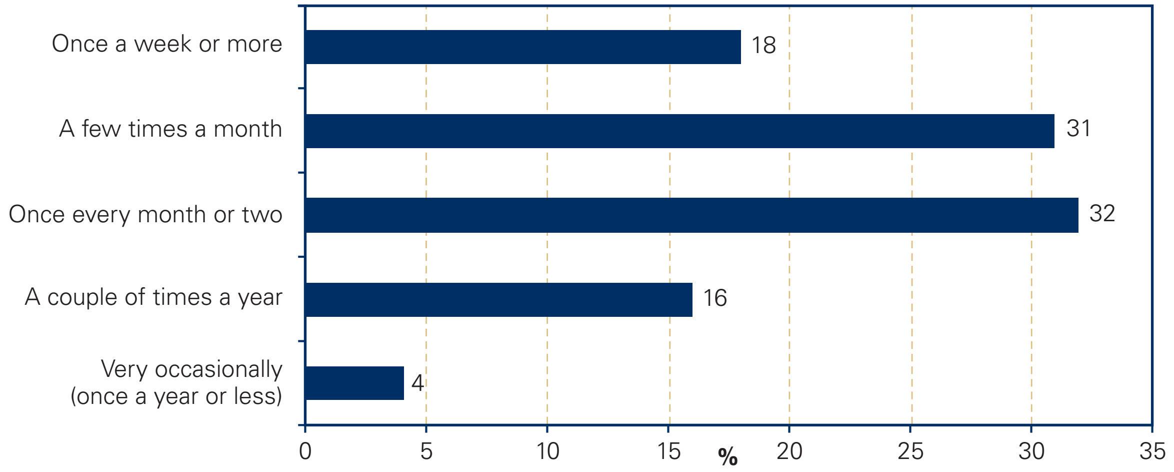
[30] Verdict (2007a).

[31] Verdict (2007a).

## How often do people shop online?

2.19. Our survey found that nearly half (49 per cent) of online shoppers bought at least monthly (see Chart 2.2). We found no major differences between the age of shoppers and how often they shopped. Male respondents shopped online more frequently than women: 22 per cent of male internet shoppers bought online once a week or more, compared to 14 per cent of females. Data from another source suggests that internet shoppers made an average of 14 online shopping 'trips' in 2006.[32]

### Chart 2.2: Frequency of Online Shopping



Source: OFT Consumer telephone survey

Base: All internet shoppers

## How much do shoppers spend online?

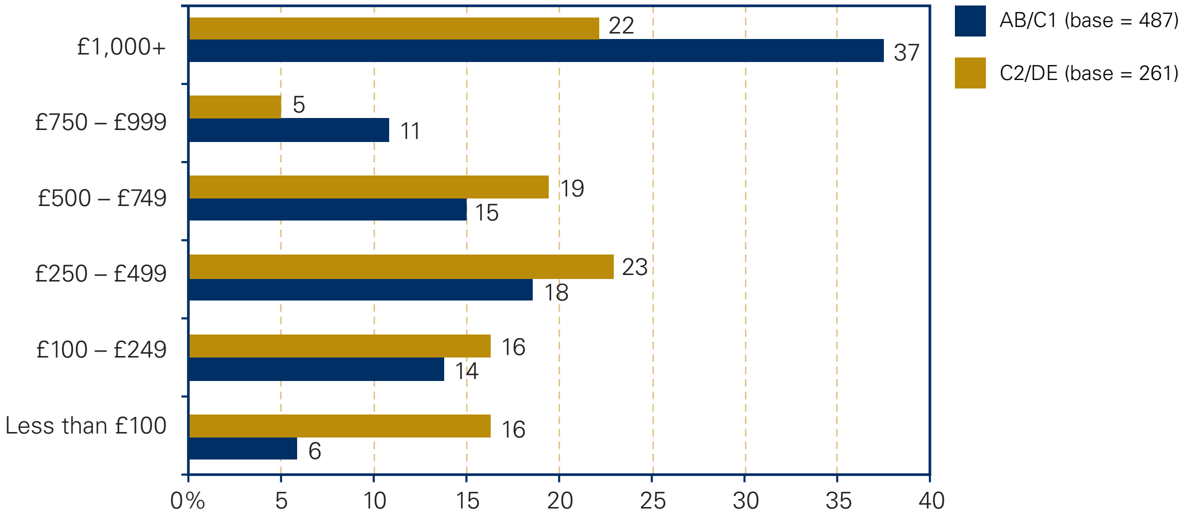
2.20. Many internet shoppers spend a substantial amount online. We estimate that the average spend was £763 in the 12 months preceding the survey, with 56 per cent of internet shoppers spending over £500 and almost a third (31 per cent) spending over £1,000. As might be expected, there was a significant relationship between age and spend: 42 per cent of internet shoppers aged 25-54 years old had spent £1,000 or more in the last 12 months, compared to only 18 per cent of over-55s and just nine per cent of under-25s.

2.21. There was also a link between social grade and online spending. Thirty-seven per cent of AB/C1 respondents to our survey had spent £1,000 or more, compared to just 22 per cent of C2/DE respondents (see Chart 2.3).[33] As might be expected, those in paid employment were more likely to be high online spenders, with 37 per cent having spent £1,000 or more; compared to 20 per cent of unemployed people. Fourteen per cent of retired people and six per cent of those in education had also spent more than £1,000 shopping online in the last year.

[32] Verdict (2007a).

[33] The established social grades referred to here are: A (Upper Middle Class, Higher managerial, administrative or professional); B (Middle Class, Intermediate managerial, administrative or professional); C1 (Lower Middle Class Supervisor or clerical and junior managerial, administrative or professional); C2 (Skilled Working Class, Skilled manual workers); D (Working Class, Semi and unskilled manual workers); E (Those at the lowest levels of subsistence, State pensioners, etc, with no other earnings).

### Chart 2.3: Amount spent online by social grade



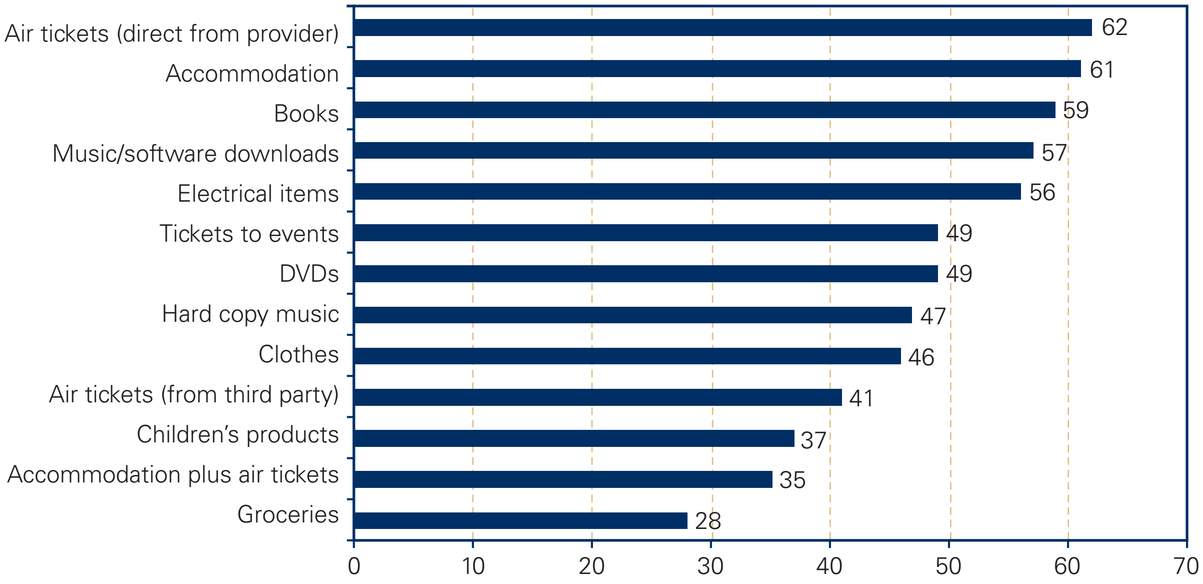
Source: OFT Consumer telephone survey

Base: All internet shoppers

### What are online shoppers buying?

2.22. In our telephone survey of consumers, holiday related items (accommodation and air tickets), books, music-related and electrical items were the most popular items bought online (see Chart 2.4). As might be expected, the nature of the product and its price influenced many shoppers.

### Chart 2.4: The products shoppers said they had bought online

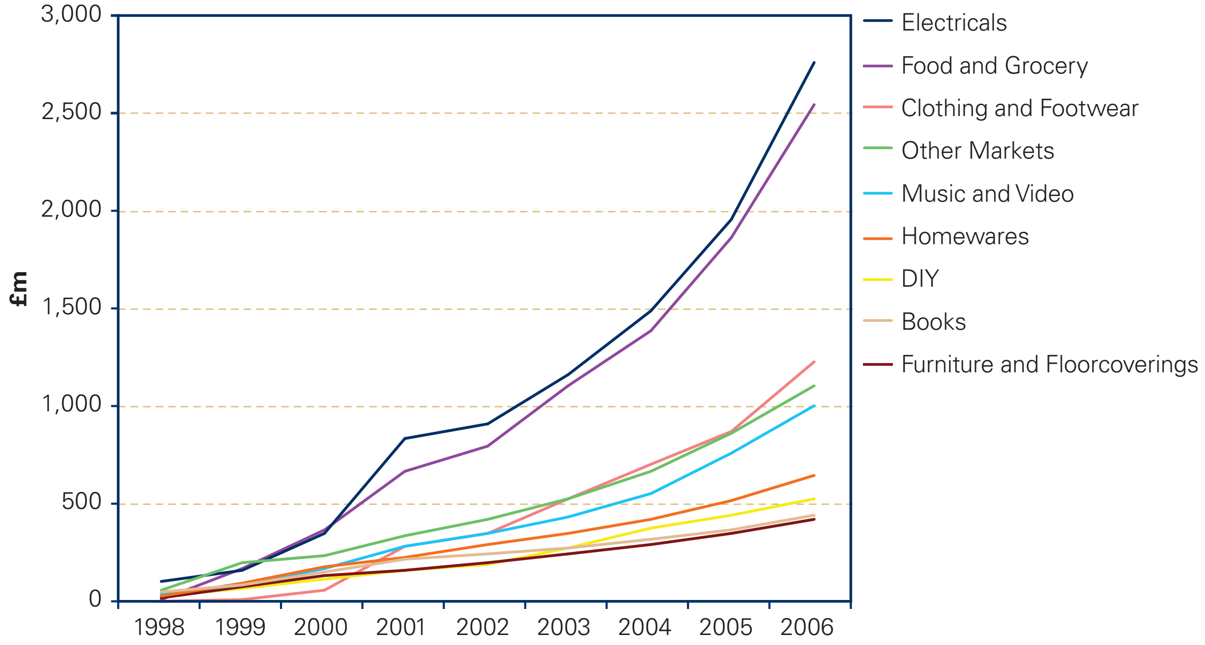


Source: OFT Consumer telephone survey

Base: All internet shoppers

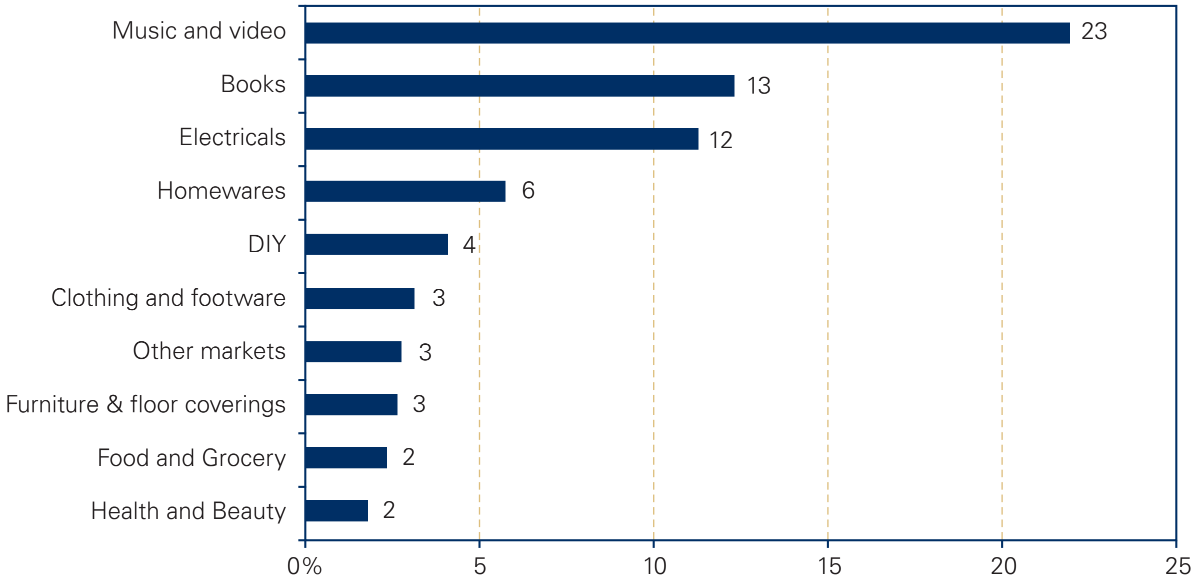
2.23. In terms of value of spend on different items, data from Verdict (see Charts 2.5 and 2.6) suggests online retail spend is greatest and fastest-growing for electrical items and groceries (although it is important to note that these figures exclude travel products).

### Chart 2.5: Online retail spend by sector, 1998-2006



Source: Verdict (2007a)

### Chart 2.6: Value of online sales as a proportion of total retail sales by sector, 2006



Source: Verdict (2007a)

2.24. In terms of our case study sectors, the approximate recent values of sales were:

- **Electrical goods:** in 2006 the value of the online retail electrical sector was £2,756 million. This was 12 per cent of all retail sales of electrical products[34]
- **Music:** in 2006, the value of online music and video[35] sales was £999 million, or 23 per cent of total sales for music and video[36]
- **Travel:** in 2005, the approximate value of online sales to households of air transport was £2,700 million[37]
- **Auctions:** a recent estimate was that purchases from online auctions using payment cards in 2005 accounted for 79 million transactions and a spend of £2.8 billion.[38]

### Who is buying what online?

2.25. There are, of course, differences in the sorts of products bought online by different types of individuals. In our telephone survey, for instance:

- Adults aged 25-54 years were more likely than older and younger respondents to have bought expensive items – particularly those associated with leisure and travel, such as accommodation and air/rail tickets
- Younger respondents (24 years and under) were significantly more likely to have bought DVDs compared to other age groups
- Respondents aged 35-44 years were more likely to have purchased children's toys
- Males were more likely than females to have bought electrical items; while females were more likely than males to have purchased clothes online.

## The implications for consumers and businesses[39]

2.26. The internet has, of course, had profound impacts on the UK economy in many ways, by enabling rapid communication and access to information, as well as prompting the development of new technologies and industries. In terms of retailing, the impacts have included greater information and transparency for shoppers to help them compare prices, products and traders; as well as new business models and products. However, when faced with deciding whether or not to sell and buy through the internet, businesses and consumers still have to weigh up its potential advantages and disadvantages over other retail channels.

### Implications for businesses

2.27. With low start up costs[40] relative to setting up a High Street shop, the internet potentially enables businesses to sell to consumers around the world at all times. It can also allow them rapidly to change their offers and to target potential customers on the basis of information they have gathered on them.

[34] Verdict (2007a).

[35] This figure combines downloads and hard copy sales. Data for online music sales alone are not available.

[36] Verdict (2007a).

[37] ONS analysis of the 2005 e-commerce Survey of Business. Note: this data represents the sales of businesses with 10 or more employees. 'Air transport' is defined by the two digit SIC '62' and is not considered the optimum for sectoral publication.

[38] APACS. See: www.apacs.org.uk/media_centre/press/06_31_07.html.

[39] This analysis draws on Frontier Economics Group (2000) and Scott Morton (2006).

[40] As found by OECD (1999).

2.28. The geographic scope of competition has been altered by the internet in some markets, increasing choice and widening competition. The extent of these impacts varies by product, because some are more suited to internet retail than others. For instance, markets for goods of known quality, such as CDs and books, may be more suited than markets for more complex, expensive, unique or rare items that buyers might prefer to inspect (such as cars and buildings) although there are certainly online markets for many such items too.

2.29. The internet has also seen the development of new products and opportunities such as downloads (music, films, games and software), photo sharing and online gaming. It has enabled the development and growth of electronic marketplaces, bringing together sellers and buyers on one platform, where potential buyers can bid for or buy directly the offered items. This has not only enabled commercial retailers to offer products for sale easily, but also allowed individual shoppers to access a marketplace for a broad range of new, second hand items and collector items. In Chapter 10, we consider one type of electronic marketplace – online auctions.

2.30. There are both potential advantages and disadvantages to businesses from trading online compared to other channels. Some of these factors are outlined in Table 2.1.

**Table 2.1: Internet retailing: Advantages and disadvantages for businesses**

| | Potential advantages | Potential disadvantages |
|---|---|---|
| **Search and choice** | • Sellers can reach a large number of customers, irrespective of location<br>• Sellers can respond to customer enquiries faster and tailor products<br>• Sellers may include a greater variety in their online catalogue, as there is no need for showrooms<br>• Sellers can quickly and cheaply change prices and other details | • Businesses need to invest in equipment, connectivity and skills<br>• A lack of physical presence mean advertising and branding are likely to be more important<br>• Low search and selection costs for buyers may mean low retention rates |
| **Interactivity** | • Sellers can receive payment from customers quickly<br>• Companies can react quickly to their customers' needs or concerns<br>• Collected data can allow targeted advertising and tailored offers | • Bad publicity may spread more quickly, so brands may be more fragile<br>• The increased importance of branding may require substantial spend on marketing |
| **Delivery** | • Businesses can easily set up, without the need for physical retail outlets (although they may still require a means to store and distribute goods)<br>• Businesses that only sell online (pure players) can locate in cheaper areas, reducing their costs<br>• Distribution costs are low for products delivered directly over the internet (such as e-tickets)<br>• Real time matching of supply and demand may reduce inventory costs | • As for other distance sales channels, companies are reliant on effective logistics as well as delivery providers |

## Online Business Models

2.31. The various ways in which businesses can sell online are complex and fast-moving. Combined with the ease of information dissemination, the relatively low cost of entry for internet retailers has facilitated a large number of new business models. Businesses may combine a number of differing practices, depending on the nature of the market they operate in and technical developments.

2.32. The three main models observed in our review of economic literature[41] and discussions with stakeholders were 'pure play', 'bricks and clicks' and sales via a third party site. According to Verdict research,[42] in 2006, of the £10.9bn internet retail spend on goods alone, £5.7bn (52 per cent) was accounted for by retailers with a physical presence ('bricks and clicks'), £3bn (28 per cent) was from mail order specialists, and £2.2bn (20 per cent) was from pureplayers.

2.33. Our review of literature found that no one model had a particular advantage, and that a firm's choice of business model depended on a number of factors, which we consider briefly in Box 2.1.

### Box 2.1: Three typical business models

- **Pure play:** In this model, the business sells purely online, or perhaps with a small number of physical sites where buyers can also visit and pick up or return products. Such retailers have been able to enter the market for a large number of goods and provide additional competitive dynamism. Pure play internet businesses may face lower staff, infrastructure and inventory costs than offline retailers.[43] In the early days of internet shopping, many commentators expected pure play retailers to dominate sales due to the lower transaction costs associated with trading online, so that shoppers would be attracted by low prices.[44] But we found that such retailers might incur additional costs in establishing brand loyalty and retaining customers (see Chapter 9). Only five pure players appeared among the biggest retailers in the top 20 most visited internet retailers listed by Hitwise in February 2007[45] and, according to the FSB, less than one per cent of UK SMEs are pure players.[46]

- **'Bricks and clicks' / Multi-channel strategy:[47]** Internet shopping has also had major implications for high street retailers. Many now also sell online and can use their existing strengths, such as their reputation, to attract people who may have concerns about shopping online; as well as networks of stores, so that buyers can pick up deliveries if they are rarely at home. Bricks and clicks retailers seem to be a relatively popular business model in the UK, if only measured by number of visits. High street retailers have entered internet retailing for many reasons – to reach more customers or to attract a new type of customer,[48] to offer a

[41] Internet Shopping – a Review of the Economic Literature – Europe Economics, OFT Paper (2007). At Annexe F.

[42] Verdict (2007b). It is, however, important to note that these figures do not take into account spend on services, such as flights.

[43] OFT by Europe Economics (2006), and OECD (1999).

[44] Steinfeld (2002), Bakos (1997), Choi, et al (1997).

[45] Hitwise/IMRG (2007) data on number of visits to their websites and OFT calculations (excluding travel sector websites, which are difficult to classify as pure play or bricks and clicks). Two of the pure players in the top ten most popular were Amazon and Play.com.

[46] FSB (2006).

[47] The top bricks and clicks retailers (excluding airline websites) by number of visits to their websites in early 2007 included Argos, Tesco, Marks and Spencer, and Next. Source: Hitwise/IMRG (2007).

[48] For example a well known high street department store has stated that its internet shop attracts younger customers than its high street stores. Mintel (2006a): One established brand found the average age of its customers fell once it went online largely due to the greater abundance of young shoppers online.

wider range of stock than is possible offline, or for marketing purposes. We heard from businesses that shoppers often browsed online and bought in store. Some bricks and clicks retailers may also benefit from their high street name since, as we discuss in Chapter 9, some people are willing to pay more to shop from a well known retailer, if they have concerns about shopping online.[49] However, while bricks and clicks have certain advantages, some research suggests that they might face higher costs from combining their existing distribution or other operations with internet retailing.[50]

- **Sales via a third party:** An interesting development made possible by the internet is the use of third party platforms, such as online auctions and other electronic marketplaces, to sell products. Our business survey found that 44 per cent of the businesses that were selling online had used such an intermediary. The third party platforms offer businesses a ready made platform that can potentially reach many more customers than a single retailer would alone. It may be relatively low cost for a new retailer to use this route. In terms of online auctions, five per cent of UK SMEs use eBay, the largest online auction platform, to sell online, which is about one quarter of all SMEs that sell online. The smallest and youngest businesses are more likely to sell via this platform.[51] There are a number of important considerations for businesses when selling via such sites, as well as those who buy from them, which we consider in Chapter 10.

2.34. Although some commentators have voiced concerns that internet sales will replace the high street, surveys of businesses are generally favourable about the impact of the internet on offline sales. In one recent business survey, 29 per cent stated that an online presence had helped boost the traditional point of sales rather than decrease it and only four per cent said that it had suffered.[52]

2.35. Furthermore, we found that many buyers still want to inspect products, or need information, advice and demonstrations. In our survey, 26 per cent of non-internet shoppers said that they did not shop online because they wanted to be able to see the goods.

2.36. Some businesses have also argued that shoppers take advantage of face to face advice before buying the item at a lower cost online, having wasted the high street shop's time. But this can work both ways. Stakeholders told us that people often reviewed information online and then bought products offline, so that they do not have to wait for them to be delivered. For instance, recent research by Royal Mail found that 30 per cent of non-home shoppers had looked at a product on a website before purchasing it in a shop.[53]

## Implications for consumers

2.37. From the point of view of shoppers, the internet has introduced some significant changes to the selection and buying process, including far greater ability to search for and buy products from anywhere in the world at any time of day; as well as easier and more rapid access to large volumes of information on products to inform their choice.

[49] This is supported by economic literature like Smith and Brynjolfsson (2001) Pan et al (2002) and Baye et al (2002).

[50] Steinfield et al (2001a), Steinfield et al (2001b), Steinfield et al (2002), Otto and Chung (2000).

[51] 'Trading on e-Bay is disproportionately concentrated amongst the smallest (0–1 and 2–4 employees, and £25–£50,000 and £50–£100,000 turnover) and youngest (0–1 and 1–3 years) businesses.' FSB (2006).

[52] GfK NOP (2006).

[53] Royal Mail (2006).

2.38. The internet provides consumers with a wealth of information from relatively accessible price information, to specialist forums where people can discuss products, suppliers and deals. Search engines and price comparison sites are potentially valuable facilitators of information which, if used effectively, can enable people to compare many products and prices and select the best deal for them – possibly at lower prices than they could otherwise find. We discuss the role and use of these search tools in Chapter 9.

2.39. Consumers can also benefit from information about products that they later buy on the high street; including advice in discussion forums and from user reviews. Provided this information is reliable, it may help to shoppers to be more informed and confident.

2.40. Although the internet offers buyers potential advantages over other channels, there are also some disadvantages compared to other channels for them to take into account (Table 2.2).[54]

### Table 2.2: Potential advantages and disadvantages for consumers

| | Potential advantages | Potential disadvantages |
|---|---|---|
| **Search and choice** | • People can shop at any time and from any location, including home<br>• Shoppers can access previously remote sellers<br>• High speed information flows can reduce search and switching costs<br>• Search intermediaries such as search engines and price comparators can provide rapid access to large numbers of retailers and products<br>• People can access information on multiple items, including user reviews and forum discussions | • People may find it hard to process large volumes of information<br>• Consumers may need to invest in technology if they shop from home, as well as develop new skills<br>• Methods of search and how results are ranked, including paid for prominence and inclusion, may not always be clear |
| **Interactivity** | • Payment details can be stored, reducing future transaction costs<br>• Buyers can leave feedback and share their views with others<br>• After-sales service (such as manuals) can be provided online | • As with other distance channels, lack of physical interaction may make it harder to assess products, build trust and achieve redress. Buyers need to trust that remote parties will treat their personal details securely<br>• Many other parties may be involved in addition to buyers and sellers (such as ISPs, search engines, product comparison sites, payment providers, delivery companies). This may lead to complications in the transaction<br>• Shoppers' preference for ease of transaction might limit switching between retailers |

[54] This analysis draws on Frontier Economics Group (2000).

Table 2.2: Potential advantages and disadvantages for consumers (continued)

| | Potential advantages | Potential disadvantages |
|---|---|---|
| **Delivery** | • Consumers do not need to leave home to shop or take delivery<br>• Buyers can sometimes track deliveries<br>• Some goods can be delivered instantly, such as downloads or e-tickets for travel<br>• A variety of delivery choices are often offered such as in-store collection or collection at a Post Office, along with services such as gift wrapping | • For delivered goods, shoppers have to wait rather than being able to take the good away immediately. For some products (such as medicines) this may not be convenient<br>• As with other distance sales channels, buyers are reliant on effective delivery and need to make arrangements to receive goods – problems with delivery can create hassle |

2.41. Some of the disadvantages to internet shopping are a feature of the 'distance' nature of the sale: consumers cannot examine the goods before they buy them, are placing trust in the trader to treat their personal and financial information securely, that they will receive the correct products and be able to resolve any problems that might crop up. In the next two Chapters, we consider the extent to which consumers have confidence in internet shopping.

2.42. The law, however, recognises some of these difficulties. Consumers shopping at a distance, including the internet, have been given additional consumer rights under the Distance Selling Regulations ('DSRs'),[55] and the Electronic Commerce (EC Directive) Regulations 2002 ('ECRs')[56] have further regulated e-commerce. We consider consumer protections, and awareness of them, in Chapter 6.

## Conclusions

2.43. The internet is a network of linked computers enabling millions of people to communicate and search for information, as well as sell and buy products. In the UK, internet access and usage has grown rapidly in the last decade, driven in part by the take up of broadband. Internet shopping has grown at a similar rate.

2.44. As a retail channel, the internet enables businesses to reach many more consumers and to sell 24/7, while shoppers can research and choose products and sellers at any time from any location.

[55] See www.opsi.gov.uk/si/si2000/20002334.htm. The DSRs were amended in 2005 – see: www.opsi.gov.uk/si/si2005/20050689.htm.

[56] See: www.opsi.gov.uk/si/si2002/20022013.htm

# 3 BUSINESS AND CONSUMER ATTITUDES

## Summary

Businesses who sell online do so to reach more consumers, and in reaction to competition from rivals. Consumers who shop online mainly do so because they consider it is convenient, it increases their choice and can help them to find lower prices. Shoppers told us that they also valued being able to access more information on products, enjoyed the process of online shopping, or bought on the internet out of necessity.

However, we estimate that 94 per cent of UK businesses do not sell online to households. In many cases they said that this was because their products were not appropriate for online sale, because of the costs involved or because they lacked the required skills. A small proportion, however, were also concerned about fraud.

We estimate that 58 per cent of people had not bought online in the 12 months to February 2006. In most cases, this was because they lacked internet access or had no desire to use the internet. However, of those who had used the internet, 33 per had not shopped online – and a lack of trust was their key reason for not doing so. Indeed we estimate that 3.4 million people were prepared to use the internet, but not to shop online because of a lack of trust or fears about personal security. Their missed savings could amount to between £175 million and £350 million each year.

Confidence and trust are important to the success of internet shopping. Forty-two per cent of businesses not selling online told us that increased consumer confidence would make them more likely to. Although many people were willing to shop online, most still had fears about doing so. For instance, 79 per cent of internet users were very concerned about the risks to the security of their payment details from online shopping. Although online shoppers seem to gain in confidence over time, even experienced ones remained worried about their financial security and privacy.

People told us that their fears stemmed from stories in the media or spread by word of mouth, their receipt of spam and phishing emails, as well as advisory campaigns and advertising. Negative media coverage is focused on spam and scams such as phishing, which could be leaving more of an impression on shoppers' views. In fact, the relationship between spam and internet shopping seems relatively limited, although some businesses that breach regulations by sending out direct marketing to consumers without their permission could be damaging confidence in the channel as a whole.

## Next steps

In later chapters we consider the importance of raising consumer and business awareness of their respective rights and obligations. We would address within future work on this, businesses' obligations under the relevant regulations not to send unwanted emails or to share their customers' information with third parties without their permission.

## Introduction

3.1. This Chapter considers the reasons why consumers and businesses use the internet to buy and sell, as well as why some do not. It examines the level of confidence in internet shopping, as well as the reasons why many people have fears about shopping online.

## Why businesses sell and consumers buy online

3.2. Although the literature identifies a wide range of factors that may persuade consumers and businesses to buy and sell online (see Chapter 2), our evidence suggested that some factors carry particular weight.

### Why businesses sell online

3.3. Put simply, businesses will usually sell online if they consider that they will make a profit from it. Every retailer's decision will, of course, be influenced by its own circumstances. For instance, some may simply be extending their existing distance selling operations, such as mail order or telephone sales. Some high street retailers may add an online sales element to their existing sales approach (to become a 'clicks and bricks' retailer) to leverage their brand name online, or if they perceive they are losing ground to competitors. And others may be new businesses: for instance, some pure players have quickly become household names.

3.4. We found there to be comparatively less survey data on why businesses sell online, than there is on why people buy online. A recent CBI/Google survey, however, found that the most frequently cited reason was to develop new sales channels (78 per cent), followed by competition from business rivals (67 per cent) and to achieve operational efficiencies (64 per cent).[57]

3.5. Similarly, our own survey results suggest that the main attraction for businesses is to reach more customers geographically, cited by 59 per cent. Other reasons given included the increasing popularity of internet shopping in general (28 per cent), the ability to sell around the clock (8 per cent), and lower costs (7 per cent).

### Why people buy online

3.6. Since the first internet shops started in the mid 1990s, large numbers of consumers have taken to internet shopping. Indeed, one study in 2005 found that approximately one fifth of internet shoppers preferred online shopping to conventional shopping.[58] There is also some evidence that many online shoppers are happy with their experience: for instance, in a 2006 survey, 71 per cent of respondents who had shopped online in the previous year reported that they were very or extremely satisfied with the experience.[59]

3.7. Our consumer survey identified convenience, followed by greater variety and lower prices as the three strongest incentives for people to shop online. These themes have also been reflected in other surveys (see Chart 3.1 and Box 3.1).[60]

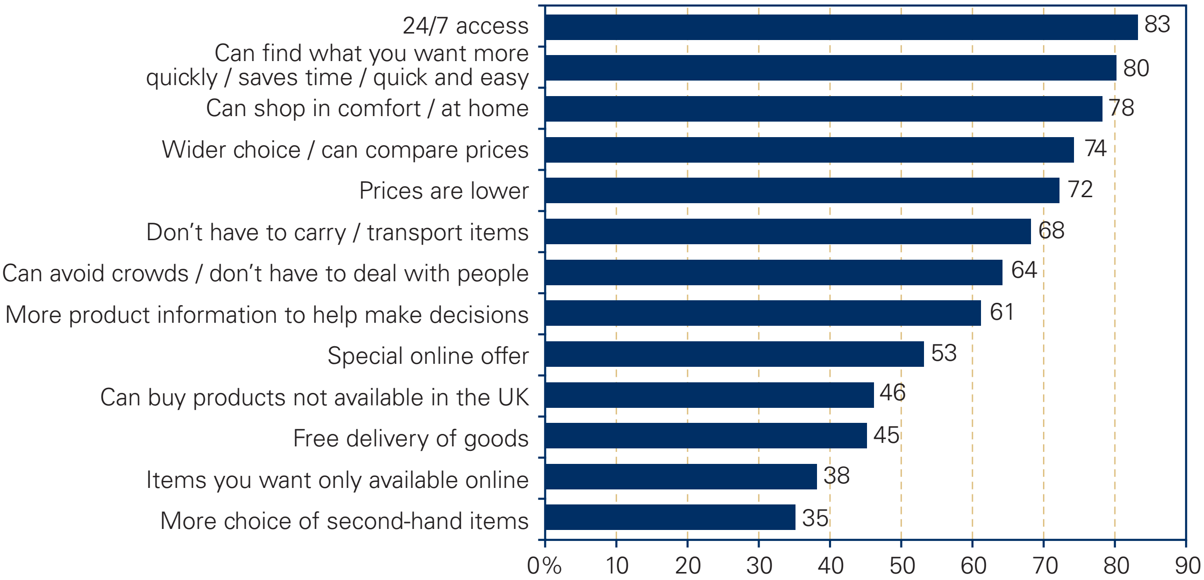
[57] GfK NOP (2006)

[58] Research by the British Computer Society, cited in OFT (2006), Internet shopping: Review of consumers' attitudes, behaviour and experience, p. 62. See Annexe E.

[59] Royal Mail (2006).

[60] The Welsh Consumer Council (Richards, 2005) found that 77 per cent of online shoppers were attracted by its convenience, while 40 per cent said that value for money or lower prices than the High Street was the reason. OxIS (2005) found that 78 per cent of respondents cited more choice of products and ease of use as the main and equally important attractions of online shopping, while 73 per cent agreed that items are more competitively priced on the internet (OxIS, 2005, p.5). GfK NOP (2006) reported that 80 per cent of consumers cited convenience, and 54 per cent cost savings.

## Chart 3.1: Shoppers' main reasons for buying online



Source: OFT Consumer telephone survey

Base: All internet shoppers

### Box 3.1: Why people shop online – the big three reasons

- **Convenience:** Our survey found convenience to be the most important factor, with 95 per cent of internet shoppers stating at least one convenience-related reason.[61] Convenience has many aspects. In particular, 24/7 access (cited by 83 per cent) and being able to find what you want quickly (cited by 80 per cent) indicate that the time saving aspect of online shopping is crucial. The other key aspect of convenience is that shoppers can avoid some of the disadvantages of offline shopping, such as having to carry items. For instance, 78 per cent of internet shoppers named 'shopping in comfort' and 64 per cent 'avoiding crowds' as key reasons why they shopped online. One focus group participant noted *'I can shop in my underpants – that is pretty convenient'*. Another commented: *'You can sit back in your house… put the details in… not having to find parking spaces, not having to queue in stores and it is done!'*

- **Choice:** The second main benefit people perceived was increased variety. In our survey, 74 per cent cited wider choice and ability to compare prices as reasons why they shopped online. Those living in rural or remote areas added that they can buy items not available nearby: *'I was after Superman swim shorts – do you think that I could get those here?'*.[62] Indeed, 38 per cent of internet shoppers said that it was the only way that they could obtain some items and 46 per cent of respondents cited being able to buy products unavailable in the UK, highlighting the reduction in market barriers brought about by the internet. This includes lower market barriers within the UK, for example for second hand items, with 35 per cent of internet shoppers indicating that online shopping gave them more choice of second hand items.

- **Perceived lower prices:** Financial motivation was also important. Seventy-two per cent of survey respondents stated lower prices as a reason for shopping online, with 53 per cent mentioning special offers and 45 per cent free delivery of goods. Shoppers in our focus groups generally thought prices were lower, citing 'getting a bargain' as a core reason for online shopping (whether prices *are* indeed lower online is discussed in paragraph 3.25 below and in Chapter 9).

[61] All of whom gave at least one convenience reason.

[62] Cited in OFT consumer focus group. See Annexe I.

3.8. Shoppers identified other reasons why they buy online, including:

- **Information:** Some focus group participants told us that they valued the diversity and comprehensiveness of product information from comparison sites, user reviews and retailers themselves (such as 360 degree scans of rooms when choosing holiday accommodation). Related to this, shoppers seem to feel that the internet has empowered them: for instance, a 2006 survey[63] found that 60 per cent of consumers believed that the internet had given them more power, while 43 per cent said that it was increasing the accountability of companies.
- **Enjoyment:** Half (51 per cent) of the internet shoppers responding to our telephone survey said that they enjoyed the online shopping experience. Particularly among heavy and frequent users, internet shopping was seen as 'recreational'. Some of our focus group participants, for instance, reported a 'buzz' from winning an internet auction.
- **Difficulties with offline shopping:** For some, their personal circumstances had made them more reliant on the internet. These factors help to underline the benefit of the internet, as well as how some come to rely on it. Three main scenarios emerged:
  - Poor choice of local shops: 37 per cent of our survey respondents said that this was one reason why they bought online. This was cited as a factor by both high and low frequency shoppers in the focus groups, and was mentioned twice as often by those in rural areas (52 per cent) as urban areas (26 per cent).
  - Transport: 16 per cent said no or poor access to their own or public transport, was one reason they shopped online. Again those in rural areas were more than twice as likely (24 per cent compared to 11 per cent) to cite this factor.
  - Personal mobility restrictions: This was cited by six per cent of respondents. One focus group participant, for instance, described how she had relied on the internet for most of her shopping needs after she had been injured.

## Why businesses and consumers do not sell or buy online

3.9. Many businesses we spoke to considered that the rapid growth of internet shopping was clear evidence of its success, as well proof of business and consumer confidence. However, most also acknowledged that shoppers, in particular, still had concerns about buying online.

3.10. Strong sales growth is clearly a positive indicator of a growing preparedness to shop online, but alone it is not a measure of attitudes or confidence. Nor does it allow us to judge whether, under different circumstances, growth could be even higher. Although internet shopping is growing faster than any other retail channel, this is in part because the growth is from a low base. Internet shopping was only three per cent of household spending during 2005 and the pace of growth in sales slowed.[64]

3.11. By value, most internet sales are made by businesses to other businesses. In 2005, Business to Consumer (B2C) sales accounted for only 21 per cent of £103bn online sales made by UK businesses, with the remaining 79 per cent being Business to Business (B2B). Furthermore, the rate of growth for B2C sales in 2005 was slower than for B2B sales: the overall value of internet sales to businesses rose by 65 per cent between 2004 and 2005, while the value of internet sales to households rose by 30 per cent over the same period.[65]

[63] GfK NOP (2006).

[64] OFT estimate based on data from Office for National Statistics (2006a) and ONS Blue Book 2006.

[65] Office for National Statistics (2006a).

3.12. We therefore explored why some businesses and consumers were choosing not to sell or buy online.

## Why businesses do not sell online

3.13. As we noted in Chapter 2, although 70 per cent of businesses had websites in 2005, only six per cent were selling online to households. While the number of businesses selling online has been growing over the last few years, penetration remains low amongst the smallest firms (with less than 10 employees),[66] which accounted for 88 per cent of all UK businesses in 2006.[67]

3.14. An FSB survey[68] of Small and Medium Enterprises (SMEs) in 2005 found that the top four barriers to take up of internet selling were:

- **Relevance** – 37 per cent of SMEs believed that internet selling was inappropriate to their business
- **Cost** – 24 per cent cited high costs of developing and maintaining a web site (and seven per cent identified connection costs as a barrier)
- **Fear of fraud** – the perceived risk of card fraud was a factor cited by 19 per cent of SMEs as preventing them from selling online
- **Lack of IT skills** – cited by 18 per cent as a barrier to online selling

3.15. Online retail is clearly more appropriate to some industry sectors than others. For instance, the FSB survey noted that 'businesses in the Health & Social Work, Construction, Mining & Utilities and Agriculture sectors were most likely to report that e-commerce was not appropriate'.[69] Furthermore, as Chapter 2 noted, the penetration of internet sales varies according to product types, with some being more suited to online selling than others. Similarly, our business survey confirmed that the main reason (cited by 22 per cent) that businesses did not sell online was that their products were not suitable (see Chart 3.2). The next most cited reasons included that they thought people preferred to see their products (7 per cent), that they only attracted a local customer base (7 per cent) and the cost of setting up security and payment facilities (seven per cent).

3.16. Trade bodies also told us that other reasons why smaller businesses in particular might not sell online included that they preferred to supply a local market, liked the social interaction of offline selling, and feared problems with delivery or not being able to meet increased demand.

3.17. In our survey, we asked those businesses not selling online what would make them more likely to start doing so. The most common answers were a reduction in set-up costs and reduction in running costs (45 per cent each), but many also cited better security (44 per cent), an increase in consumer confidence (42 per cent) and lower risk of fraud (42 per cent).

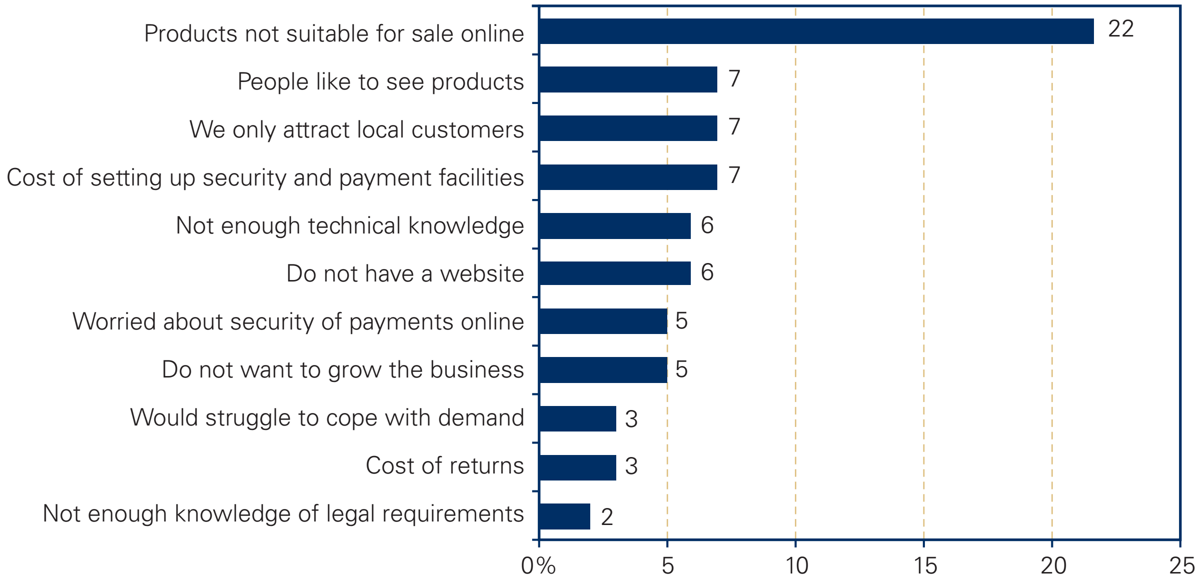
[66] In 2005 the methodology for the ONS Annual e-Commerce Survey was changed so it no longer sampled businesses with less than 10 employees. In the 2004 survey, the proportion of businesses with less than 10 employees selling online to households and/or to businesses was around 6 per cent compared to 12 per cent for those with more than 10 employees.

[67] ONS Interdepartmental Business Register 2006.

[68] FSB (2006).

[69] FSB (2006).

**Chart 3.2: Reasons why businesses do not sell online**



Source: OFT Business telephone survey

Base: All businesses that do not sell online

3.18. Nineteen per cent of SMEs in the FSB survey cited perceived risk of card fraud as a factor preventing them selling online. In our survey, however, only five per cent of those not selling online said that fears about the security of taking payments online was deterring them. Five per cent were worried about the security of payment/e-crime and seven per cent were deterred by the cost of setting up security and payment facilities. However, one in five businesses (22 per cent) felt that their products were not suitable for online selling or stated a broad range of more personal 'other' reasons (27 per cent) separate to security and fraud.

3.19. More in line with the FSB survey were the responses from those businesses we interviewed who do sell online, but do not take payments online. One third (33 per cent) of these indicated that they did not take payments online because they were worried about the security of payments and e-crime. And one in five (21 per cent) said that the costs of setting up security and payment facilities were a barrier to taking payments online.

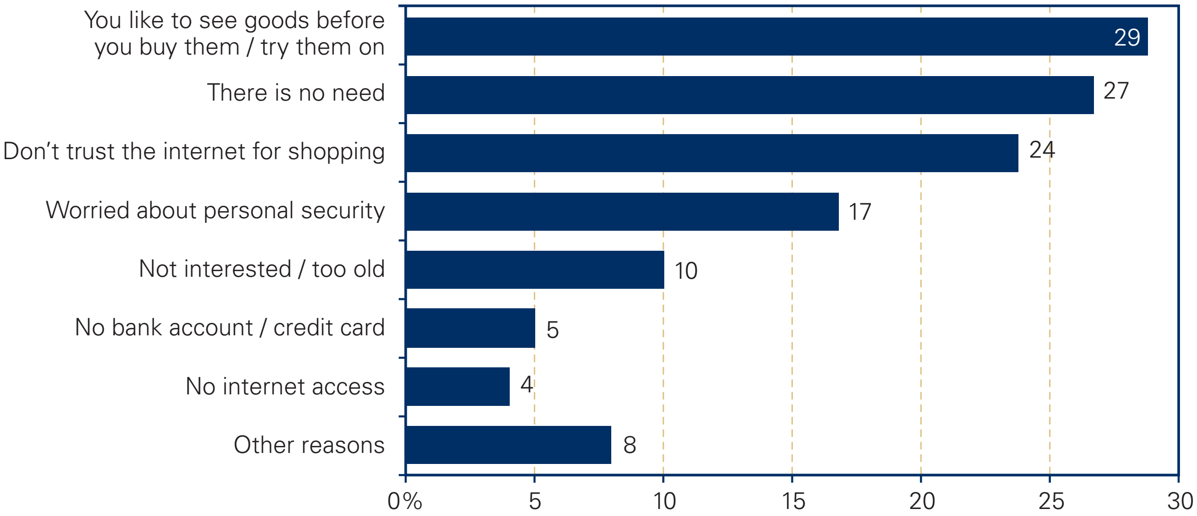
## Why people do not buy online

3.20. For most people who do not buy online, this is simply because they do not use the internet: 38 per cent of the total adult population had not used the internet in the 12 months to April 2006.[70] However, focusing just on those people who had used the internet during that period, two thirds (67 per cent) had shopped online and one third (33 per cent) had not shopped online. This implies that 42 per cent of the total adult population (or 20.4 million people) shopped online in the 12 months to April 2006.

3.21. We asked those people who had used the internet in the 12 months to November 2006, but had not used it to shop, why they had not done so (see Chart 3.3). The reasons they gave mainly related to a preference for offline shopping, or a belief that the internet had nothing new to offer: 'I like to see the goods/try them on before I buy them' (29 per cent) and 'there is no need – there's nothing you can't buy elsewhere' (27 per cent).

[70] OFT estimate based on Office for National Statistics (2001-2006).

### Chart 3.3: Reasons why people who had used the internet had not shopped online



Source: OFT Consumer telephone survey

Base: All non internet shoppers

3.22. In focus groups, participants mentioned a range of reasons for not shopping online, including the need to touch, see or try on a product and assess the quality, which made some reluctant to buy clothes or expensive electrical items online. The idea of having to be at home and potentially take time off work to wait in for a delivery was also a strong barrier for some participants.

3.23. However, trust also emerged as a key issue: in our survey, 24 per cent of internet users who had not shopped online did not trust the internet for shopping, while security concerns were also mentioned by 17 per cent. In fact, when combined, lack of trust/worries about security online were the most common factor deterring internet users from shopping online, cited by a total of 34 per cent.[71] Looking at the potential pool of all internet users (see Chart 3.4), this means that just over one in ten people (11 per cent) with internet access who could shop online are being put off by fears about security. This equates to 3.4 million UK adults.[72]

3.24. It is clear that shoppers' fears about online payment security risks are considerable. Indeed, we found that many were willing to pay more for peace of mind. In our survey, one-third (32 per cent) of concerned internet shoppers and non-shoppers indicated that being concerned about the security of an online transaction had meant that they bought a product offline even though the price was higher.

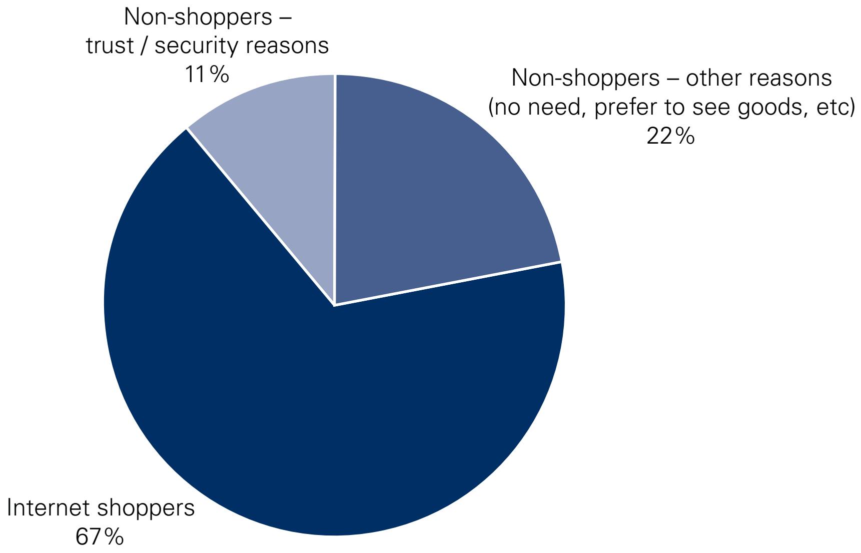
3.25. Lack of confidence has economic impacts. Using recent Which? studies, which found that prices were lower online,[73] each deterred shopper could save between £52 and £104 per year if they shopped online in a similar pattern to the average internet shopper. In total, all those internet users that do not shop online because of privacy and security concerns could save between £175 million and £350 million per annum in aggregate compared to shopping offline, with the lower figure assuming that new internet shoppers only capture half the potential savings.

[71] Consumers could give more than one response to this question and so the response categories are not mutually exclusive. Note that the four per cent of people who responded that they did not have internet access are likely to represent people who use the internet but would not have access to enable purchases (for instance, they used it at work).

[72] Other recent surveys suggest that the figure could be higher than this. For instance, Get Safe Online (2006a) reported that as many as 18 per cent of people will not shop online because of fears of online crime.

[73] Which (2006) and Which (2007). Price differences of 12 per cent in the market for electrical items and of 16 per cent in the travel sector have been found. See Chapter 9 for more discussion of online prices.

### Chart 3.4: Internet users who do and do not shop online



Source: OFT Consumer telephone survey & Office for National Statistics (2006c)

Base: All internet users

## Understanding consumer confidence

3.26. Almost all the stakeholders who commented told us that trust and buyer confidence were crucial to the success of online shopping. While many took the view that growing sales demonstrated confidence in the internet as a retail channel, most acknowledged that even those people willing to shop online still had concerns about doing so. We therefore looked into the issue of confidence in more detail.

3.27. We found that 86 per cent of internet users in our survey had at least some concerns about shopping online, while only 12 per cent had no concerns.[74] Although 59 per cent of internet users felt that the benefits of shopping online outweighed any concerns they might have, 37 per cent disagreed or strongly disagreed with this suggestion.

3.28. However, the majority (71 per cent) also felt that shopping through mail-order had the same or less risk than shopping online, and broadly equated the risk of internet shopping to buying over the telephone (50 per cent agreed it was as safe). Although 77 per cent thought buying from a doorstep salesman was less safe than over the internet, nearly one in five (19 per cent) felt it was as safe as or safer to buy from a doorstep salesperson than online.

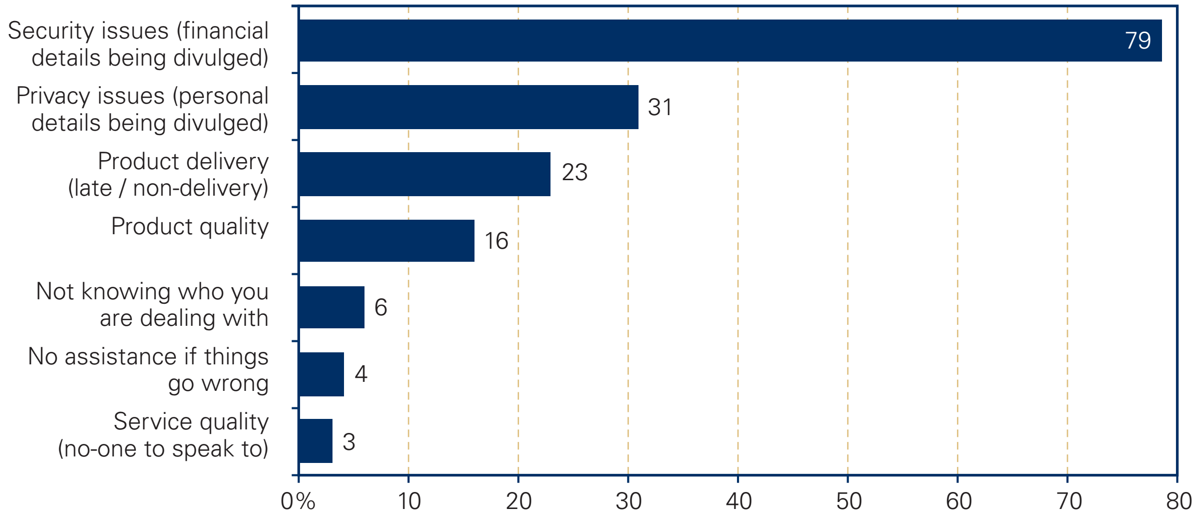
### What do shoppers fear?

3.29. In our survey, 79 per cent of internet users told us that having financial details divulged was a concern, while 31 per cent were concerned about divulging personal details (see Chart 3.5). In comparison, product delivery was a concern for 23 per cent of these respondents and the quality of the product was a concern for 16 per cent. Lack of interaction was rated as a key concern by less than ten per cent of respondents.[75]

[74] Note that ‘internet users’ refers to internet shoppers and non-shopping internet users. In our telephone survey of consumers, ninety per cent of ‘internet users’ were also internet shoppers (as set by quota). See Annexe H for further explanation.

[75] The categories were: ‘Not knowing who dealing with’, ‘no assistance’ or ‘service quality issues’.

**Chart 3.5: Concerned shoppers – what do they fear?**



Source: OFT Consumer telephone survey

Base: All internet shoppers, and non shoppers who are concerned about the security of the internet and who have any concerns

3.30. In our focus groups, participants raised concerns about the employees of retailers being more likely to steal details or funds online rather than over the telephone because of the greater anonymity:

*'The telephone feels more real – I am talking to a real person and I trust them more'* (Non shopper / lapsed, Newcastle, younger)

3.31. Those with more knowledge about the internet reported the notion of personal information being accessed by a third party or many third parties as the major source of their security concerns and fears:

*'It's more difficult for people to commit fraud with a physical card because of chip and pin so they are moving over to the internet'* (Internet shopper, Croydon, younger)

3.32. Respondents told us that they were most concerned about their financial details being divulged – more so than they were about having personal details more generally being divulged (although this was also a substantial concern). Although security and privacy issues are closely related, there are some noteworthy distinctions:

- Security issues tend to focus on use of the financial payment details given in making transactions online
- Privacy concerns are broader and usually relate to how businesses treat wider personal information, ranging from email addresses to medical information.

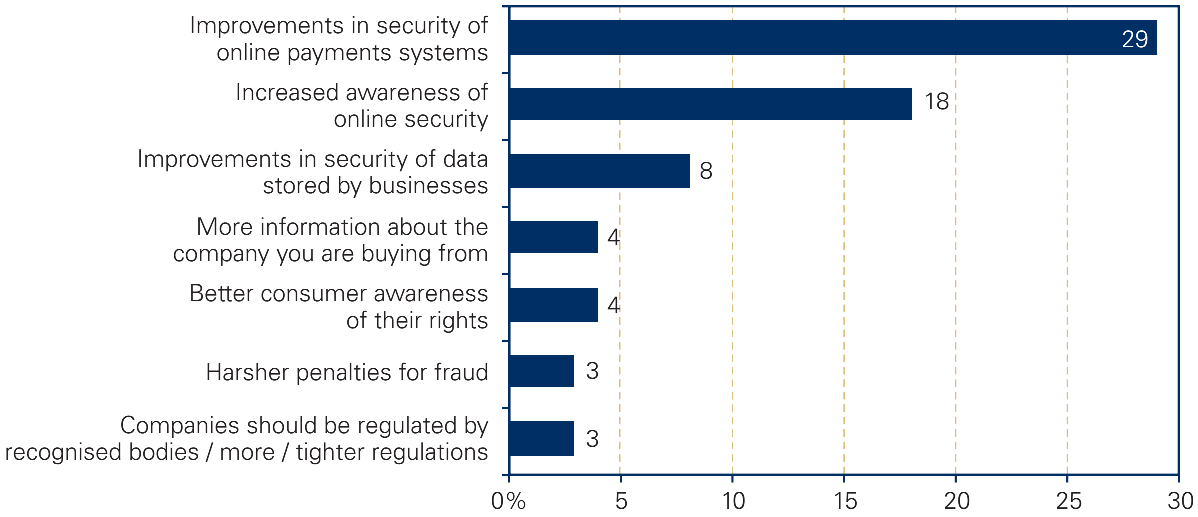
3.33. Ofcom's recent Media Literacy report[76] noted the relative difference in the way people view personal and financial data, confirming that people are particularly worried about losing personal financial data (such as credit card details). While 54 per cent of users were happy to enter a personal email address on the internet, only 28 per cent of users said they were likely to disclose credit card information on the internet.

[76] OFCOM (2006).

3.34. Likewise, the Information Commissioner's Office (ICO) most recent survey[77] of individuals found that financial data was considered the most sensitive personal information (88 per cent), ahead of health information (72 per cent) and personal contact details (68 per cent).

3.35. Businesses seem well aware of the strength of shoppers' fears – particularly in relation to paying online. Those we spoke to, as well as respondents to our survey, said that the main ways to improve confidence in online shopping required improving security of payment systems; the awareness of online security; and the security of stored data (See Chart 3.6).

**Chart 3.6: What do businesses think could be done to improve consumer confidence?**



Source: OFT Business telephone survey

Base: All businesses in the electrical, travel and music sector and those selling via online auction sites

## Why are shoppers so concerned about security and privacy?

3.36. The extent of fears about online security was highlighted in a recent survey[78] which asked which of a series of crimes individuals felt most at risk of in their everyday lives: 21 per cent of those who never buy online identified internet crime, which was higher than burglary (16 per cent) or mugging (11 per cent).

3.37. Research literature[79] suggests that all 'remote' shopping generates buyer uncertainty about product quality, delivery, financial risk, and communication in the event of problems. The types of concerns are relatively similar for all distance selling channels. But the literature also suggests that the internet has *amplified* shoppers' perceptions of the risks of potential financial security and confidentiality problems from the sharing of personal information.

3.38. Stakeholders who commented on the strength of people's concerns about security and privacy risks suggested that they reflected a combination of 'fear of the unknown', 'loss of control' and 'worries about the potential impacts of data loss'. Enforcers at our workshop considered that one of the main implications of internet shopping for consumers was that it required not only skills to make a purchase, but also a new level of understanding of technology and protection that some people adapted to more easily than others, leaving others feeling more uneasy.

[77] ICO (2006a).

[78] Get Safe Online (2006b).

[79] Internet Shopping – Review of Consumers' Attitudes, Behaviour and Experience. See Annexe E, Section 3.

3.39. Our literature review found that research on attitudes to internet shopping has been mainly limited to large-scale quantitative surveys, rather than the qualitative work needed to understand the reasoning behind their fears, such as depth interviews and focus groups.[80] However, our focus groups suggested that perceptions of the potential impact of the disclosure of financial and personal details were an important explanatory factor. For instance, the hassle involved in recovering from 'a scam' or identity theft, which was perceived as a risk when online shopping, was a powerful reason to not shop online: participants begrudged having to relearn a new pin, remember a new credit card number or change banks.

3.40. Research by the Information Commissioner's Office (ICO) has found that 87 per cent of people equated the loss of personal information with threats to their safety and health.[81] CIFAS research[82] also suggests that victims of identity theft might spend three to 48 hours of work clearing their name. However, in many instances the issues could also be resolved with a phone call to their bank: over half of their respondents spent less than 24 hours rectifying the situation, 16 per cent took one to two hours and 12 per cent three to four hours (although in 11 per cent of cases it had taken over a week). About half of the victims said that their experience had had a big impact on their stress and health levels, and slightly more claimed that it caused them great inconvenience.

## What generates shoppers' fears?

3.41. Shoppers told us that it was mainly stories from the press, as well as those spread by their friends and family that was making them concerned about shopping online (see Chart 3.7). However, receiving spam and phishing emails[83], as well as advice and advertising were also major reasons why they felt worried. We concentrate on the impact of the media and spam below, and consider the role of security advice and advertising in the next Chapter.[84]

[80] Internet Shopping – Review of Consumers' Attitudes, Behaviour and Experience. See Annexe E, Section 3.

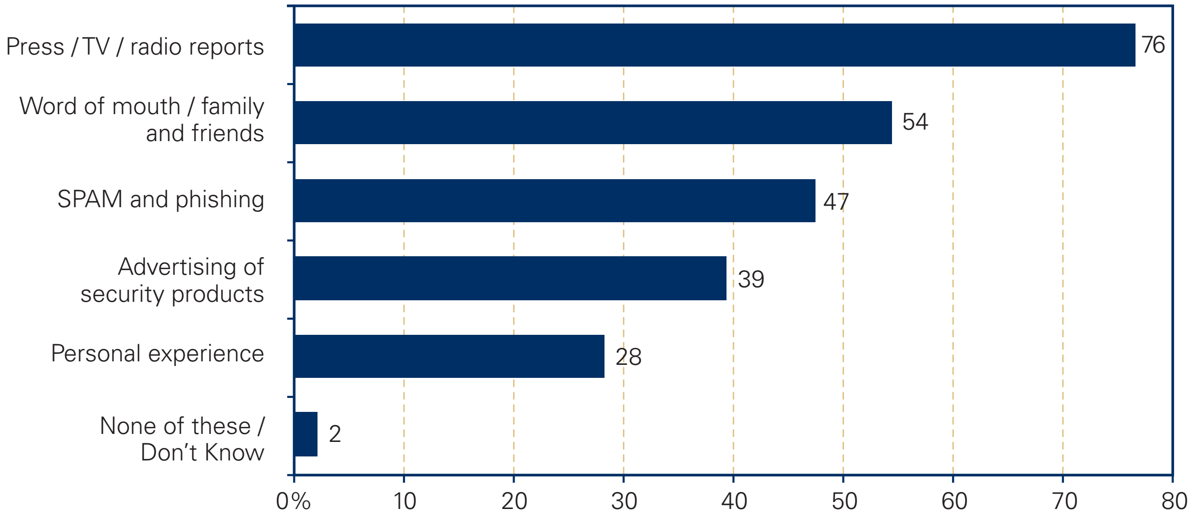
[81] www.ico.gov.uk/upload/documents/pressreleases/2006/annual_track_press_release.pdf

[82] CIFAS, the UK's Fraud Prevention Service is a not for profit membership association dedicated to the prevention of financial crime. See: www.cifas.org.uk/reports_what_about_the_victim.asp

[83] Spam is electronic junk mail. 'Phishing' is a form of spam which attempts to dupe individuals into revealing sensitive information to fraudsters (see Chapter 4).

[84] In our survey, 54 per cent of respondents cited 'word of mouth/family and friends' as generating their concerns. We could not tell what issues they had discussed, but assume that they were likely to have included media stories, as well as personal experiences such as receiving spam. In the survey, 28 per cent also cited personal experience. Again, we could not tell what these were, although they may also have related to receipt of spam, as well as wider problems from shopping online such as with delivery. We consider in Chapter 4, the extent to which they had experienced problems relating to security and privacy.

### Chart 3.7: What factors generate shoppers' concerns?



Source: OFT Consumer telephone survey

Base: All internet shoppers, and non shoppers who are concerned about the security of the internet and who have any concerns

## The role of the media

3.42. Seventy-six per cent of shoppers who had concerns said that their fears stemmed from press, TV or radio reports. This was a view shared by some participants in our focus groups:

*'I always hear bad stories in the media, which is a shame because the internet is a great way to shop'* – older, Cardiff, Internet shopper

3.43. Many organisations we spoke to thought that media coverage of internet shopping often fuelled the public's fears unnecessarily. This perception was confirmed by our surveys of consumers and businesses. In our business survey, 46 per cent of those that considered people were less confident buying a product online than in business premises said that concerns about online shopping came from the media, compared to only 26 per cent who said that they came from personal experience.

3.44. Given the widely held view that the press was generating most concern, we commissioned an analysis of media reporting of internet shopping issues over the five months from October 2006 to February 2007.[85] This found that, by volume, most coverage (56 per cent) was neutral and 31 per cent was positive. The higher proportion of positive stories, focused on the benefits of internet shopping as cheaper, convenient, growing and innovative. Only 13 per cent of coverage was negative – mainly addressing related issues of fraud, scams, spam and phishing, but also after sales care issues. There were no major differences by media type (tabloid, broadsheet or broadcast).

[85] Online Shopping Media Evaluation Report, TNS (2007). An analysis of nearly 300 stories in the national press and broadcast coverage, during five sample weeks. See Annexe D.

3.45. We cannot be sure why there was an apparent discrepancy between the perceived negative effects of press coverage and the analysis we commissioned.[86] However, possible explanations include that readers may be more likely to read and remember negative stories – particularly where they perceive that the story is about a threat that could affect them personally. Negative coverage also appeared to be focused on a small number of specific issues (spam, phishing and fraud), potentially meaning that these were more memorable than the more diffuse range of positive stories.

3.46. There is academic literature which has uncovered factors which affect people's perception of risk. One study[87] found that dramatic but uncommon events bias people's judgement in favour of that event occurring. Coupled with the media's tendency to stress this type of event, few but dramatic negative stories can outweigh more numerous, but more mundane, positive stories.

3.47. Finally, some stakeholders also suggested that there may have been a shift in recent times towards more neutral or positive reporting:

*'I haven't heard of any issues recently about online trading. There was a bit of a spate in the news last year about it but I think that's died down'* (National travel business)

## Spam and phishing emails

3.48. Of the other generators of concern, the receipt of spam and phishing emails was perhaps most significant, since our media analysis found that a high proportion of negative media stories centred on these issues and because they may feature in the 'personal experiences' cited by some concerned consumers. Spam, sometimes known as electronic junk mail, is the general name given to unsolicited emails. Most spam is an attempt to sell a service or product, but some is intended to trick recipients out of money or to hand over personal details ('scam spam'), and some is to deliver malicious content (such as viruses).

3.49. Every internet user with an email address is likely to have been sent spam. In 2006, 86 per cent of all emails were identified as spam, up from 81 per cent in 2005 (although down from a peak of 95 per cent in July 2004).[88] For most email users, the bulk of spam is filtered out by their ISP, but a spate of 'image spam' which evaded these filters recently led to more reaching email account holders. The growth in the number and variety of 'phishing' emails (a form of scam spam which seeks to dupe individuals into revealing personal and financial information to fraudsters), has also brought the issue to the fore.[89]

3.50. Spammers 'harvest' email addresses from various sources, such as social networking sites or make 'dictionary attacks', using software that creates billions of permutations of possible addresses. Spammers can be very difficult to trace as they tend to work through 'bots', or 'robot networks', which are networks of illegally 'hi-jacked' computers through which spam is routed. However, what tracking is possible suggests that most spam originates outside the recipient's country, with sources scattered across the globe.[90]

[86] The media analysis study was conducted over one week periods per month from October 2006 to February 2007 inclusive. It may be that the tone of reporting differed during the weeks not monitored, as negative stories are usually generated by an event sparking a short term rise in reporting. The time of year (Christmas) may also have had an influence on the results of the press analysis, although the period covered ran from October to February. There was some evidence that the volume of positive and neutral stories were more evenly matched in January and February (but even in this period there were more neutral and positive than negative stories).

[87] Tversky and Kahneman (2002).

[88] MessageLabs (2006).

[89] Phishing is a crime under section 2 of the Fraud Act 2006

[90] Some sites maintain updated statistics and mapping of spam sources. See for instance: www.postini.com/stats/index.php or www.spamhaus.org/statistics/countries.lasso

3.51. In response to its growth, there has been significant industry and international attention paid to the fight against spam, with the creation of several fora. These include the Messaging Anti-Abuse Working Group and the London Action Plan (LAP), which was an initiative of the International Consumer Protection Enforcement Network (ICPEN) that brings together the private sector and public enforcement agencies. The OECD Task Force on Spam has also developed a Spam Toolkit, and provides background resources and materials, as well as a list of national focal points for enforcement authorities.[91] See Chapter 11 for more discussion of some key international developments.

3.52. Given the ways spammers work, and in the view of most organisations we asked, it seems unlikely that shopping online substantially increases the spam received by internet users and it is unclear why receiving spam and phishing emails should make people particularly wary about shopping online. However, two possible explanations are that recipients may fear their computer has become unsafe because of spam, or that if they shop online they will receive unwanted emails.

3.53. In terms of receiving emails that might compromise a computer, a small amount carry malicious code[92] and recipients who suffer problems with software applications on their computers due to inadvertently downloading such programmes may consequently be worried about using the internet generally, or fear that they have downloaded software that could steal their personal details if they use them online (including to shop). Chapter 4 discusses these risks and some ways consumers can avoid them.

3.54. Another potential link between shopping online and receipt of unsolicited emails is that shoppers may receive direct marketing emails from businesses from whom they have bought, or who have obtained their details during negotiations to buy their products, even if they have not given their express consent to receive such communications. Consumers may also find that they receive direct marketing from third party businesses as a result of businesses passing on customer details for marketing purposes. However, this should only be the case if they have given their consent.

3.55. The relevant regulations here include (see Box 3.2):

- the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECRs'),[93] which cover unsolicited direct marketing messages sent by a range of methods including emails
- the ECRs, which, amongst other things, require advertising emails to be clearly identifiable as advertisements
- the Data Protection Act 1998 ('DPA') which amongst other things, requires businesses to have consumers' consent before sharing their personal details.[94]

[91] See: www.oecd-antispam.org/

[92] In 2006, 1.5 per cent of emails (one in every 68) in the UK contained a virus or Trojan (down from 2.8 per cent in 2005) and 0.36 per cent (one in every 274) contained a phishing attempt. MessageLabs (2006).

[93] The PECRs are enforced by the Information Commissioners Office (ICO). Detailed guidance is provided by the ICO at www.ico.gov.uk.

[94] See ICO (2006b).

### Box 3.2: Regulations protecting consumers against unwanted emails

**The PECRs:** Under the PECRs, businesses need consent from recipients before they may send direct marketing emails. However, there is an exception to this general rule which is often referred to as the 'soft opt-in'. Under the soft opt-in, businesses which have obtained a person's email contact details in the course of the sale or negotiations for the sale of a product or service (for example by asking for a quote) may send direct marketing emails to that person. However, the marketing must be in respect of similar products and services only and the recipient must be given a free and simple means of refusing the use of their contact details for marketing purposes when the details are initially collected and at the time of each subsequent communication. This is often achieved by means of an opt-in or opt-out box when future emails are sent. Failure to do this will be a breach of the Regulations.

In addition, the PECRs prohibit solicited and unsolicited direct marketing emails which conceal or disguise the sender's identity and those which do not include a valid address (like an email address) to which the recipient can send an opt-out request. Individuals can opt out of receiving such messages at any time by contacting the business sending them. The business must comply with an opt-out.

**The ECRs:** These apply to, amongst others, businesses which advertise or sell goods or services by email. Those businesses must comply with the ECRs as well as the PECRs. Their advertising emails must be clearly identifiable as advertisements, identify the business they have come from and any promotional offers and their terms. Where they are unsolicited, those emails must be clearly identifiable as unsolicited advertising without the recipient even needing to open them.

**The DPA:** Under the DPA businesses must use personal information fairly and lawfully. In broad terms, this will mean telling people how they will use their personal information at the time it is collected (in other words that the business may in future send direct marketing emails about its products) and obtaining at least their implied consent to such uses. Whether consent may be implied will depend on the circumstances. An individual is entitled to send a business a written notice requiring it to stop, or not to start, using his personal information for the purpose of direct marketing. When a business receives such a notice, it must comply as soon as it can. There are no exceptions to this.

Consumers may also receive direct marketing from third party businesses as a result of businesses passing on customer details for marketing purposes. However, this should only be the case if they have given their consent. Again, DPA is relevant. In broad terms, businesses which collect email addresses to pass on to other organisations for marketing purposes, must tell consumers to whom it is proposing to pass the details, what sort of products and services they will be offering and obtain consent.[95] Again, the ability to opt-out at any time applies.

3.56. However, there is evidence that some businesses may be in breach of the PECRs: recent research[96] found that 31 per cent of the top 200 companies across 13 sectors were not compliant with the regulations. This was almost the same as a similar survey two years before.

[95] See ICO (2006b).

[96] See www.cdms.co.uk/articles.asp?articlekey=87.

3.57. In our survey of businesses, just under half (49 per cent) with websites said that they did not gather any information from consumers who visited their sites. However, a third (33 per cent) gathered the email address of visitors, a quarter logged the pages viewed or the name of the visitor (26 and 25 per cent respectively) and one in five (21 per cent) gathered the postal address of the visitor. Of those gathering information, 43 per cent used it to promote special offers or items which may be of interest (39 per cent), while 16 per cent used it to tailor prices to individual customers. In the follow up interviews, some businesses said that they used transaction data to target customers themselves but none of them sold it onto third parties.

3.58. Nevertheless, our analysis of websites found that it might not always be clear to users whether they needed to opt in or opt out of sites sharing their information with third parties for marketing purposes. Different reviewers sometimes drew different conclusions when looking at the same site. Lack of clarity in businesses' policies on sharing customer details may affect confidence among those considering whether to shop online. The ICO, for instance, found that only 16 per cent of people were confident that internet sites treated their personal information properly; 52 per cent were concerned that their details may be shared.[97]

3.59. Any campaigns to help business awareness of their obligations therefore, need also to include advice on this issue, to make sure that businesses do not:

- send marketing emails to people with whom they have no commercial relationship or who have not consented to receive them
- share shoppers' personal data with third parties without their permission.

## How experience of online shopping affects confidence

3.60. Many stakeholders suggested that lack of confidence in online shopping would be self-correcting, as the pool of experienced shoppers grew. In interviews, businesses often suggested that in the long term, young people who had grown up with the internet would be more confident:

*'As a new generation of people that have grown up with the internet become the main consumers, there will be increased confidence'* (National Travel Agent)

3.61. We did find that people who had been shopping online for longer tended to feel more confident about doing so. For instance, our telephone survey revealed that respondents who had been shopping online for two years or less were more concerned about security (92 per cent) than those who had been shopping for 3-6 years (84 per cent) or seven years or more (76 per cent). Nevertheless, even experienced online shoppers registered high rates of concern.

3.62. Likewise, in the focus groups, newer online shoppers were generally more likely to be concerned about shopping online, with one novice describing an internet purchase as a:

*'…nerve-racking experience – one I would not want to go through again'* – younger, Croydon, internet shopper

3.63. We also found some encouraging evidence that people felt that the internet was becoming a safer place to buy. In January 2006, 69 per cent agreed or strongly agreed that the internet was becoming a safer place to shop, with more internet shoppers agreeing than non-internet shoppers (79 per cent and 42 per cent respectively).[98]

[97] ICO (2005).

[98] Consumer Omnibus Survey Report, January 2006. See Annexe K.

3.64. However, our surveys did not support a generational difference in confidence, with no significant differences in confidence across age groups. Furthermore, it was not clear that people's perceptions of risk diminished if they were making more frequent or regular purchases online. We found that even the most experienced of internet shoppers often still had concerns: there was little difference in levels of concerns when considering the four different experience profiles of regular shopper/infrequent shopper and large/low spender.

3.65. Also, it did not seem that shoppers' biggest and most specific concerns about security and privacy faded as they spent more frequently. Indeed, respondents who shopped online more than once a month were significantly more likely to be concerned about security issues, when compared to those who shopped once every month or two (84 per cent compared to 72 per cent). Although these people were shopping despite their fears, they were still worried; and indeed their concerns appeared at least in part to relate to their perceived exposure to risk.

3.66. Given that security and privacy concerns seem to be the main factor deterring internet users from shopping online, as well as a continuing worry even for experienced shoppers, we consider in the next Chapter the risks and protections available.

## Conclusions

3.67. Although internet sales have been increasing for years, this does not necessarily mean that they are growing as much as they might. There are many reasons why businesses and shoppers might not want to use the internet to buy and sell, including lack of internet access, products not being appropriate, or simply no desire to use it. However, we also found that some were being deterred by concerns about using the internet as a retail channel, and although many people were willing to shop online, most had fears about doing so.

3.68. The fears could be acting as a drag on the growth of internet shopping. We estimate that 3.4 million people were prepared to use the internet, but not willing to shop online because of a lack of trust or fears about personal security. Their missed savings could amount to between £175 million and £350 million each year. Although online shoppers seem to gain confidence over time, even experienced ones remained worried about their financial security and privacy.

3.69. Although the media is seen as the chief generator of concerns, most coverage is neutral or positive. However, negative coverage is often focused on spam and scams such as phishing. In practice, the link between these threats and online shopping may be limited, but some businesses that breach regulations by sending out direct marketing to consumers or sharing their information without their permission, could be damaging confidence in internet shopping as a sales channel.

### Next steps

3.70. In later chapters we consider the importance of raising consumer and business awareness of their respective rights and obligations. We would address within future work on this, consumers' rights not to receive unwanted emails or to have their information shared without their permission.

# 4 SECURITY AND PRIVACY: RISKS AND PROTECTIONS

## Summary

The organisations we spoke to told us that people's fears about internet shopping were understandable, given the relatively unfamiliar and fast evolving nature of the internet, and were likely to be influenced by regular stories about new threats. However, many also thought that shoppers' worries about buying online were excessively high.

Internet card fraud has grown rapidly since the introduction of chip and PIN on the High Street, although this growth is largely in line with the growth in internet shopping. There is a lack of reliable data on the prevalence and significance of the risks from internet shopping itself. However, some of the dangers commonly associated with internet shopping may be more a result of data lost offline or through general internet usage, rather than the result of having shopped online.

Nevertheless, there are risks attached to using the internet, and to selling and shopping online, which need to be taken seriously. To guard against risks to their businesses and to address consumers' concerns (which put some off shopping online altogether), it is in traders' best interests to consider the range of technical and other protective measures they can take.

Likewise, online shoppers can reduce risks by taking precautions and watching for warning signs. Provided they do so, it seems unlikely, at the time of writing, that they will be at substantially more risk than if they use other means of buying at a distance. Even if online shoppers experience the fraudulent use of their payment card details, they have regulatory protections which means that they are unlikely to have to pay anything.

However, public awareness of these precautions and protections remains weak, despite campaigns and numerous sources of advice. Many people also do not recognise that they need to take some responsibility for their protection online, believing that this is solely the role of businesses and other organisations.

Awareness campaigns, as well as commercial advertising may also be scaring people away from shopping online as much as they are informing them. Some level of concern may helpfully encourage people to be vigilant, but campaigns need to be balanced, so that shoppers know how to protect themselves, without having excessive fears about online shopping.

## Next steps

We want to work with interested parties in this field to encourage the development and provision of more accurate ways of assessing the risks of online shopping. We also want to work with them to ensure that shoppers have an accurate view of the risks and know how to protect themselves, and that businesses are encouraged to provide a safe shopping environment. We also want to raise awareness of what shoppers can do if something goes wrong.

## Introduction

4.1. The previous Chapter identified that consumers and businesses most fear risks to payment security and personal privacy from e-commerce and that these concerns are at least as great and may be greater for internet shopping than other distance channels. However, almost all the organisations and businesses with whom we discussed this issue claimed that while the level of concerns about these potential risks were understandable, they were likely to be disproportionate to the real risks.

## What types of risk do consumers and businesses face?

4.2. Internet shopping can involve potential risks to consumers and businesses. Risks to consumers broadly revolve around the possibility of personal and financial information, such as addresses, passwords and credit card details, being compromised. The primary risk for businesses is that information is used fraudulently to make a purchase from them. If businesses are responsible for the loss of consumers' data, they also face damage to their reputation, as well as a possible fine.

4.3. The following section outlines some of the ways in which personal and financial information can be compromised. In trying to assess these risks it is important to draw a clear distinction between those that are directly related to internet shopping, and those which involve the internet in some way, but may have less direct connection to the process of shopping online.

4.4 Almost everyone is potentially at some risk that their personal data might be acquired and used fraudulently online, whether or not they use the internet. The anonymity of the internet, and the easy access it provides to a growing and wide range of retailers, as well as high value goods, makes it an attractive place for fraudsters to use stolen card details. This is especially the case since the rollout of chip and PIN, which has increased the security of 'cardholder present' transactions. While card fraud in the High Street has fallen by 67 per cent in the last two years, card-not-present (CNP) fraud[99] has grown by 74 per cent since 2003, to become the largest type of card fraud in the UK. Most (73 per cent in 2006) of this CNP fraud took place over the internet.[100]

4.5. However, figures for card fraud tend to describe where card details were used, rather than where they were compromised. Card details can be obtained in many ways that do not involve the internet. Furthermore, several organisations told us that certain kinds of security incidents involving the internet, could be mistakenly associated with internet shopping by shoppers. This could have the effect of exaggerating perceptions of the risks involved in internet shopping. With this in mind, we draw the distinction between three types of risk, the latter of which is perhaps most relevant to our discussion of internet shopping:

- Risks which can affect anyone whether or not they use the internet
- Risks which may arise from using the internet
- Risks which may arise when shopping online

### Risks which can affect anyone whether or not they use the internet

4.6. Almost everyone is potentially at some risk that their personal data might be acquired and used fraudulently online, whether or not they use the internet.

[99] CNP fraud involves stolen card details being used to pay for goods or services over the internet, by phone or mail order.

[100] Source: APACS (2007).

### Offline acquisition of data leading to fraudulent use online

4.7. APACS, the main source of data on card fraud, told us that it was not always possible to be sure how details had originally been acquired, but that most personal and financial data were compromised offline. In our consumer survey, just over half (56 per cent) also considered that credit card details were most commonly obtained offline.

4.8. There are many ways in which a third party might acquire personal and financial data offline from data holders (individuals, traders, financial institutions, government, etc), which might then be used fraudulently online.

4.9. Some possibilities include the loss or theft from data-holders of paper-based data (such as from bin-raiding, information lost in the post, or poor disposal of confidential waste). Or they may suffer physical loss, or theft, of data maintained on a computer or other data storage device, such as a flash drive or mobile phone. Rogue traders or employees of legitimate businesses may acquire and misuse personal and financial information supplied offline by trusting consumers (for example, by skimming cards). Or individuals may lose information to scams, through fake surveys, or readers hidden in ATMs. There have also been some high profile offline data losses by organisations. The most recent widely reported example involved the theft of a laptop containing confidential data from an employee of Nationwide bank.[101]

4.10. Such scenarios are not new. Nor do they have a direct relationship to online shopping from the perspective of shoppers. Individuals may be exposed to these risks even if they have never used the internet, let alone shopped online. However, where data stolen offline are used to commit fraud online, there is a danger that consumers may associate this with internet shopping, potentially damaging the reputation of the internet as a retail channel.

### Online acquisition of data collected from offline use

4.11. There are also circumstances in which the online acquisition of sensitive information by malicious third parties may be seen as related to internet shopping, despite sometimes having little or no link. For instance, many firms keep information about their customers on databases which could be subject to hacking attacks via the internet. These data are likely to concern people who have shopped offline as well as those who shopped online.

4.12. In a recent high profile example, credit and debit card details were hacked from the servers of TJX (the parent company of retailer TK Maxx).[102] While the internet clearly played a key role in facilitating this data acquisition, we understand that TK Maxx has never sold online in the UK. However, the involvement of the internet may mean some people incorrectly associate this with internet shopping.

## Risks which may arise from using the internet

4.13. The risks described above relate to situations where non-users of the internet may find their data being used fraudulently online. People who use the internet but who may or may not shop online potentially expose themselves to other risks. Key examples include the receipt of phishing emails, and the sharing of personal information online.

[101] Nationwide were fined for this incident by the Financial Services Authority (FSA) under the Financial Services and Markets Act 2000.

[102] Press releases from TJX which relate to this incident can be found at: www.tjx.com/tjx_message_tk.html.

### Scamming emails and phishing

4.14. Phishing attacks can dupe individuals into revealing personal and financial information to fraudsters. A typical phishing attack involves fraudsters sending out emails purporting to be from a bank, which ask individuals to follow a link to a replica website and 'confirm' their details. These are attempts to trick people into handing over important personal and financial details. Modern technology allows these scams to be conducted quickly and on a mass scale, with official websites and logos reproduced perfectly, and emails sent at random to huge numbers of people at once.[103]

4.15. Many organisations told us that phishing was probably the most significant online risk. An AOL survey[104] found that 48 per cent of UK internet users had received emails aimed at tricking them into revealing bank account details, and APACS reported a growth in incidents of phishing websites being set up of over 1,400 per cent between January 2004 and June 2006,[105] albeit from a low base. MessageLabs found that phishing emails rose slightly from one in 304 emails in 2005 to one in 274 in 2006.[106] APACS have stated that: 'the surge in phishing attacks is mainly due to banks and internet companies getting better at quickly identifying and closing down phishing sites, which has meant fraudsters have naturally increased the number of attacks.'[107]

4.16. As we noted in Chapter 3, 47 per cent of concerned shoppers cited receipt of spam/phishing emails as a reason for their concerns about internet shopping. While it is clear that phishing is a risk to internet users, much of it is unlikely to result from internet shopping.[108] On the whole, anyone with an email address is likely to be sent phishing emails, whether or not they have shopped online.[109]

### Sharing of personal data online

4.17. Some individuals share a surprising amount of personal information in blogs and on social websites. This can provide a fruitful resource for fraudsters who aggregate personal information from multiple sources with the intent of misusing an individual's identity; a tactic known as 'phoraging'.

## Risks which may arise when internet shopping

4.18. There are, however, also opportunities for potential fraudsters to acquire personal and financial data as a result of, or during, online activities that could relate to internet shopping. Data can for instance be taken either from the consumer themselves, or from a business holding their details. We have not conducted a comprehensive audit of all risks, but some examples of each kind include:

[103] Organisations can also experience phishing attacks. 'Spear phishing' attacks frequently target employees of a company, pretending to be from the HR or IT department, requesting information that will allow a hacker to access a corporate network.

[104] YouGov (2005).

[105] www.apacs.org.uk/media_centre/press/06_07_11.html.

[106] MessageLabs (2006).

[107] www.apacs.org.uk/media_centre/press/22.09.06.html

[108] There is a chance that some businesses might share customers' email addresses with third parties so that they reach an eventual perpetrator of a phishing attack.

[109] For a description of some of the techniques used to generate email addresses for phishing or spam emails, see Chapter 3.

## Online acquisition of data from consumers

**Interception of data in transit**

Secure socket layer (SSL) is a security standard which encrypts data and transmits it along secure connections. The widespread use of SSL (see below) means that the majority of connections through which data passes are encrypted, and secure. However, if consumers are shopping with one of the few websites which does not use SSL, then data in transit may potentially be vulnerable.

It is also possible that third parties in range of a wireless network might eavesdrop on information as it is passed over the air. However, most wireless modems allow data to be encrypted, which reduces this risk. Additionally, sensitive information should only be entered over a secure (SSL) connection.

**Malicious software**

Malicious software (malware) can be used to compromise the security of information stored on, or entered into a computer.[110] Some stakeholders have argued that poorly secured always-on broadband connections have significantly increased the vulnerability of users to malware.

Malware can be bundled into, or falsely appear to be, a seemingly harmless application which the consumer downloads and activates (a 'trojan'). Spam email can contain trojans. Vulnerabilities in web browsers can also be used to install malware when visiting complicit or hijacked websites. Malware comes in various forms and can lead to data compromises in several ways. For instance:

- 'Key logging' software which records the keystrokes made on a computer, can capture personal and financial information as it is entered by consumers when they log in to a website, or complete a transaction. McAfee noted a 250% increase in the number of keylogging malware packages between January 2004 and May 2006.[111]
- Unencrypted data which is stored on a computer[112] may also be vulnerable to 'spyware', which can search a hard drive for personal and financial information, and send it back to a potential fraudster.
- 'Session hijacking' occurs when a hacker takes over a legitimate session between two machines, once it has already been authenticated.

[110] The security industry has monitored threats of this kind, and worked to raise awareness of them, for some time. For recent examples of threat assessments, Postini (2007), or McAfee's Security Insights (www.mcafee.com/us/security_insights/default.html).

[111] McAfee (2007). Banks have been addressing this risk through the use of drop down menus to enter data

[112] It is possible that this information could be stored in cookies. Cookies are small text files which are created on a user's hard drive when they log into a site.

### Online acquisition of data from businesses holding consumers' details

| | |
|---|---|
| **Hacking of corporate networks** | Data holders such as businesses and financial institutions can be targeted by criminals seeking to steal information (often financial data) by hacking into customer databases. This is a growing concern for any business which stores consumer information on networks, regardless of whether it received this information online or offline.<br>Just like attacks on consumers' computers, these hacking attacks on corporate networks frequently originate from a piece of malware. In one of the most high profile cases, a trojan was installed onto a server of the US payment card processing company, CardSystems Inc, in September 2004. This reportedly resulted in the compromise of 40 million credit card accounts, with fraud on a minimum of 250,000 accounts. |
| **Insider Fraud** | Transactions involving payment cards bring the risk that untrustworthy members of a trader's staff may in some circumstances be able to gain access to customers' financial details.<br>Businesses we discussed this with claimed that online transactions posed less of a potential risk than for other distance sales due to the common use of payment mechanisms which only send traders payment confirmation, and not the full card details. However, online payment systems do not always protect the privacy of financial information in this way, and not all online traders take payments online.<br>Also, the ease with which a website can be set up means that it can sometimes be difficult for consumers to gauge the trustworthiness of the trader they are buying from. |

4.19. It is also worth noting that there is a general risk attached to using public computers or public wireless networks (for instance, in libraries or internet cafes). A public computer may not be free from malware and a wireless network may not be encrypted. As a result, it is generally recommended that personal information that might be used in online shopping, such as passwords and card details should not be entered into a public computer or public wireless network.

## The significance of these risks

4.20. The above list of risks associated with internet shopping is not exhaustive, and new variants regularly emerge. Given the potential range of possible new threats, their rapid evolution, their profile in the media and perceptions about their impacts, it is hardly surprising that security and privacy are ranked as the main consumer concerns. This section considers evidence of how significant the risks actually are.

## Problems in measuring online risks

4.21. There are limitations to how accurately the magnitude of online risks can be measured. Internet security is a technically complex, fast-evolving area, where it is hard if not impossible to disentangle the relationships between issues such as data protection, identity theft and e-crime.[113] As a result, attempts to quantify the risks involved in shopping online face various difficulties, including:

- Any technical assessment is quickly rendered obsolete by the rapidly changing nature of the risks involved.
- There is a lack of reliable data to enable an assessment of risk. This was highlighted in some of the submissions to the House of Lords Select Committee on Science and Technology Inquiry into the wider issues surrounding Personal Internet Security. It has also been highlighted by the OECD as a global issue.[114]
- Survey data on experiences is often unreliable, because many consumers may not know the nature of the risks or be aware that they have experienced risk. When consumers suffer fraud, it is often not possible for them accurately to determine whether their data was compromised online or offline.

4.22. Acknowledging these limitations, we will consider three sources of evidence of the scale of the risks involved in shopping online: stakeholders' views, survey evidence and data on financial losses.

## Stakeholders' views

4.23. Although some interests may wish to play down the risks, the message we received was generally consistent across a range of parties. For example, APACS and businesses we discussed this with felt, almost unanimously, that information passed over the internet was highly secure. Some suggested it was more secure than that passed over other distance selling channels.

4.24. In its evidence to the House of Lords, the British Computer Society stated 'there is no known case of a credit card being intercepted while being sent on the internet'.[115] One major online retailer also told us that *'we have not had a single case of a customer contacting us as a result of having had their credit card data fraudulently used following a transaction…'*.

## Evidence from consumer surveys

4.25. It is very hard to measure with any certainty shoppers' experience of fraud from online shopping, because this requires them to know how their personal data were acquired. Survey findings in this area vary quite substantially. For instance, a recent Get Safe Online (GSOL) survey stated that six per cent had suffered fraud while shopping online in the past 12 months, but also that this was the same number of people who had had their bag or wallet or mobile phone stolen, or their home broken into.[116]

[113] For a discussion of the problems in measuring fraud see ACPO (2007).

[114] OECD (2005c), p.29.

[115] BCS (2006), p3.

[116] Get Safe Online (2007).

4.26. In comparison, we found that two per cent of the online shoppers we surveyed had experienced misuse of their personal or financial information in the preceding twelve months. But this figure may also overstate experience of fraud, because respondents may have been including non-fraud issues, such as personal details being misused by companies sending them unwanted emails.[117] Just under two per cent of businesses told us that the complaints they received regarding online sales most commonly concerned online payment security issues.

4.27. Direct comparisons between data on consumer perceptions, and that on the actual instance of security problems illustrate some of the limitations of consumer surveys in this area. For example, recent research in the US by Mintel[118] found that over a third of respondents saw the internet as the place where identity fraud was most likely to take place, and 68 per cent were either 'very concerned' or 'somewhat concerned' that their credit or debit card details would be stolen if they shopped online. But a survey of fraud conducted by the Better Business Bureau[119] found that 63 per cent of U.S. fraud in 2006 occurred at the hands of friends, family or neighbours and involved lost or stolen wallets, cards and cheque books, unauthorised access to computers, and stolen mail or rubbish.

## Evidence from reported financial losses

4.28. The scale of financial losses is also often used as a proxy for the extent of risk online. Estimates of total financial losses online vary widely,[120] and can include significant losses incurred by security breaches that may have no real bearing on the security of internet shopping, such as denial of service attacks.[121]

4.29. Research which measures internet card fraud is more directly relevant to internet shopping. APACS report that internet card fraud in 2006 totalled £154.5m.[122] Looking at the UK according to their data on payments, the level of CNP fraud over the internet in 2005 was 0.41 per cent of the value of online transactions in that year, which was higher than the level of fraud on CNP mail order and telephone transactions for the same period (0.18 per cent). In contrast, the level of fraud on all other transactions was 0.09 per cent.[123] This seems consistent with the established view that the internet is a very attractive place for fraudsters to use stolen card details, as discussed in paragraph 4.4. It also emphasises the importance of traders using good security measures, as we discuss below.

4.30. Internet card fraud is also increasing in value – albeit at much the same rate as the growth in online spending, so that as a percentage of sales it has remained relatively stable. For instance, APACS told us that online losses grew by 32 per cent between 2005 and 2006 (£117m to £154.5m)[124] slightly lower than the 37 per cent growth they recorded in card spending online over this period (£22bn to £30.2bn).

[117] TNS Omnibus Survey – on behalf of the OFT. This figure is backed by other research, such as Mintel (2005), which also reported that two per cent of internet users claimed to have experienced theft of personal and/or financial details online.

[118] Mintel. Security and ID Theft – U.S.

[119] BBB and Javelin (2006).

[120] For instance, see the range of values estimated by the different surveys quoted in OECD (2005c).

[121] Denial of service attacks aim to make a resource, typically a company website, unavailable to legitimate users. This is commonly achieved by overwhelming a website with traffic from a large number of 'zombie' computers which have been infected by a virus ('botnets'). They can involve attempts to claim a ransom.

[122] APACS (2007).

[123] This figure relates to fraud involving retailer transactions, and excludes cash withdrawals from ATMS, or from bank counters.

[124] APACS (2005).

4.31. While these data demonstrate that fraudulent spending on the internet is a growing problem and underline the importance to businesses to guard against it, they do not show where shoppers' card details came from in the first place. APACS's view is that much of this fraud originates offline rather than from online shopping, and that 'the incidence of computer hackers stealing and using cardholder data from websites is very low'.[125]

## Security and privacy: Protections and redress

4.32. For any of the above risks to be realised, a third party with malicious intent needs firstly to acquire personal information, and then to be able to use these data. There are three key sets of protections available with which consumers and businesses can reduce these risks, and gain redress if anything goes wrong:

- Technical protections against malicious data acquisition
- Technical protections against fraudulent use of data
- Regulatory protections and redress

### Technical protections against malicious data acquisition

4.33. A range of technical solutions is available to help consumers and businesses guard against the risks that relate to internet use or to internet shopping, as described above. A comprehensive account of such protections is impossible since new ones are being developed all the time as new threats emerge, but examples include:

| | |
|---|---|
| **Scamming emails** | A growing number of technical solutions to phishing are available. Anti-phishing toolbars are increasingly becoming standard on web browsers. For instance, Microsoft's Internet Explorer 7 warns users if the website they are visiting is a reported phishing site. Likewise, eBay's Account Guard system is intended to protect against spoofs and phishing.<br>However, with or without technical protections, scamming emails ultimately rely on deception, so consumer awareness and care is key to defeating it. |
| **Interception of data in transit** | The risk of data in transit being intercepted or altered is extremely low. Secure socket layer (SSL) is a security standard which encrypts data and transmits it along secure connections.<br>Consumers should always check that a connection is secure by looking for a padlock symbol, or the prefix 'https' to the website address. |
| **Malicious software** | In order to protect against security risks, consumers need to be aware that a computer which is connected to the internet requires continuous maintenance. Malware often exploits vulnerabilities in the software already on a computer, including the operating system.<br>• When these vulnerabilities are identified, the vendor of the software usually releases a patch to fix them within a short period of time. Keeping up to date with these security patches can substantially reduce the probability of malware infecting a computer. |

[125] APACS (2007).

- Anti-virus software can further reduce the likelihood of a security breach, but since new viruses are created all the time this also requires continual updating.

Further technical protections can include:

- The use of a personal firewall can alert the user when outgoing connections are being attempted, and can provide intrusion detection.
- Ensuring wireless networks are protected with encryption and that access is restricted to known computers.
- There are also specific technical solutions aimed at specific threats. For instance, in response to key loggers, many banks are to roll out two factor authentication (see below).

Perhaps most importantly, there are also simple behavioural steps that consumers can take to guard against these threats. These include:

- Avoid opening emails with attachments from unknown senders and if in doubt do not open any ‘executable’ attachments (for example, those that end in .exe or .zip).
- Avoid downloading or running applications from untrusted websites
- Use different passwords for different accounts

**Hacking of corporate networks**

This is primarily an issue for businesses, and not something consumers can address directly. Mastercard, VISA, American Express and Discover have recently implemented the Payment Card Industry Data Security Standard (PCI DSS). This sets minimum technical (for example, firewalls, encryption) and non-technical (for example, access policies) standards for data security.[126]

The PCI DSS is mandatory for any organisation using the cards of any of the above suppliers, which stores, transmits or processes cardholder account and transaction data.

**Insider fraud**

There is a range of measures consumers can take to reduce risks when sharing details with an unknown trader over the internet.

- Most simply, consumers can contact them to confirm their identity. Trader’s websites are required to include contact details by the DSRs and ECRs.
- Clicking on the padlock symbol allows users to check the SSL server certificate, which verifies who owns the server, and the certificate issuer. There are currently industry initiatives to build on the padlock symbol to make the signals clearer to consumers. For instance, Enhanced Validation SSL Certificates turn the browser’s address bar green when visiting a registered site and displays information on the certificate holder and issuer. When visiting a website known to be fraudulent, the address bar turns red.
- When card details are entered at the point of purchase, the question of whether the trader gets access to these details depends on how the payment system is integrated into their online shop. Whether the details are shared with the trader may not be clear to the shopper, although some alternative online payment systems make clear that they allow consumers to complete a transaction without revealing financial details to the trader.

[126] The twelve key requirements of PCI DSS can be found at: www.Visaeurope.com/aboutVisa/security/ais/requirements.jsp. More information is available from www.pciforum.us/pci/default.aspx.

4.34. In summary, when shopping online, basic measures that consumers can adopt to protect themselves include:

- avoid sharing personal information on social websites that might be used fraudulently
- stay alert for scamming emails and do not open emails with attachments from unknown senders, nor open links or attachments if in any doubt about the email
- do not download or run applications from websites you are not certain you can trust
- use security software and keep it up to date
- look for a padlock symbol, or the prefix 'https' to the website address when sharing personal information, and click on the padlock symbol to check the certificate
- ensure wireless networks are protected with encryption and that access is restricted to known computers
- avoid entering personal information into public computers or wireless networks
- contact your bank immediately if you think your personal details have been disclosed.

## Technical protections against fraudulent use of data

4.35. Stakeholders suggested that the introduction of chip and PIN had significantly increased the security of transactions where the cardholder is present, such as those on the High Street. As a result, however, card not present (CNP) transactions have become a more attractive target for fraud than they previously were.

4.36. If a credit card is stolen and fraudulently used to make a purchase from a trader, the card issuer will usually charge the value of the sale back to the trader. Consequently the industry has been developing initiatives to help reduce traders' exposure to fraudulent CNP transactions. These include:

- Payment service providers often offer automatic fraud prevention software which screens transactions, flags unusual payments, and checks the number and type of recent transactions on a card. Such software can also be purchased independently by retailers.
- The payment card industry is also combating online card fraud by adding to the information requirements needed to make a transaction. For instance, the Address Verification Service (AVS) requires the consumer to enter their registered address, which is then checked against the address details held by the card issuing bank. Similarly, some websites require the consumer to input the three or four digit number printed on the back of the card, the Card Security Code (CSC), which is then validated. While this can help combat some kinds of CNP fraud (for instance, where details have been 'bin raided'), the fact that this information is printed on the card is a limitation.
- 3-D Secure technology is a relatively recent innovation, intended to raise the standard of authentication required for online transactions. The two most common implementations of 3-D Secure technology are Verified by Visa and MasterCard SecureCode. During a transaction involving a participating merchant, the consumer is required to enter a passcode to authenticate their identity directly with the issuing bank. If a transaction has been authenticated using 3-D Secure, any liability for chargebacks shifts from the merchant to the issuing bank.
- The next development in this area is likely to be two factor or token based authentication. This involves the use of a hand held card reader which generates a

unique one-time only (dynamic) passcode when the chip card and pin are entered. The use of a card reader to generate a dynamic code should significantly reduce the impact of keyloggers, since even if a passcode is captured, it will expire, and be useless once the consumer has used it once.

## Regulatory protections and redress

4.37. Consumers are also protected by a regulatory framework which provides redress mechanisms in case anything goes wrong. In terms of protecting consumers, businesses also have an obligation under the Data Protection Act 1998 (DPA) to retain and process personal data securely. See box 4.1.

### Box 4.1: Data Protection Act 1998: 'personal data must be secure'

The Data Protection Act (DPA) provides a framework to ensure that personal information is handled properly. Businesses which process personal information must comply with eight principles. The seventh principle is that personal data, including financial data, must be secure.

The seventh data principle requires a data controller to take 'appropriate' technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.[127]

In terms of what is 'appropriate', this will depend on the circumstances but the DPA expressly requires that the level of security must be appropriate to the harm that might result from non-compliance. A data controller must therefore consider what harm is likely to result, for example, from the unauthorised disclosure of personal data such as credit card details.

In determining what measures are 'appropriate' the state of technological development and the cost of implementing the measures are also taken into account, and, if the data controller has employees who have access to personal data, the data controller must take steps to ensure the reliability of these employees.

The Information Commissioner ('IC') states that the data controller must take a 'risk-based' approach to what measures are appropriate, and that management and organisational measures are as important as technical ones. The IC guidance sets out some security controls that the data controller is likely to have to consider.[128]

Insofar as personal data are processed not by the data controller but by a person on his behalf (a 'data processor'), there are additional obligations on the data controller, notably that the data processor chosen must provide 'sufficient' guarantees in respect of the technical and organisational measures and must take reasonable steps to ensure compliance with those measures. However, even when using a data processor, the data controller retains responsibility for the data.

4.38. Furthermore, consumers may be concerned that their card details may be intercepted and used fraudulently. However a consumer will not have to pay anything if their debit or credit cards (or card details) are stolen and used in a distance contract, for example to buy goods on the internet. See Box 4.2.

[127] DPA Schedule 1 Part II paragraph 9; IC Guidance paragraph 3.7.

[128] IC Guidance paragraph 3.7.

### Box 4.2: Theft and unauthorised use of card/card details

Shoppers are protected from financial loss in the event of the theft of their credit or debit card (or card details) by a combination of the DSRs,[129] The Consumer Credit Act 1974[130] and the Banking Code.[131]

Where fraudulent use has been made of a consumer's card in connection with a distance contract, they are entitled to be re-credited with all sums paid. It is for the card issuer to prove that the use was, in fact, authorised by the consumer.[132] These protections apply to the use of a 'payment card' which includes not only credit cards but also charge cards, debit cards and store cards. The position is the same if the card details, and not the card itself, are stolen.

In most other circumstances a customer's liability is similarly limited as long as the card is in their possession – and where the card is lost or stolen, the maximum liability is £50.

## Awareness of protections

4.39. A wide range of technical and regulatory protections are available for online shoppers and traders. However, these are only effective if consumers and businesses know about them and put them to use.

### How aware are consumers of possible protections?

4.40. Evidence suggests that consumers' awareness and usage of protections are too low. But many consumers also seem not to be aware that they need to take sensible precautions online. Get Safe On Line (GSOL) found that only 24 per cent of people consider it their own responsibility to safeguard themselves online, and 41 per cent thought that big online companies should insure their customers against fraud.[133] Some consumers may therefore be increasing their exposure to risk unnecessarily.

4.41. For instance, as we noted above, a computer that is connected to the internet requires ongoing maintenance to prevent security compromises. However:

- APACS found that only 46 per cent of people regularly updated their anti-virus software, and only a third had a firewall.[134] GSOL found that 46 per cent do not have anti-spyware, and 35 per cent do not download security updates.[135]
- GSOL also found that 83 per cent of people had anti-virus protection on their PCs, but a fifth had not updated it in the previous month.[136] Indeed, these figures may overstate the actual protections in place: in a 2004 survey, 71 per cent of consumers with virus protection said they updated it daily or weekly, but a scan of their computers showed that 67 per cent had not been updated in the past week.[137]

[129] Regulation 21.

[130] Section 83 and Section 84.

[131] From 1 March 2005, this is a voluntary Code which establishes standards to which most banks, building societies and credit card companies have agreed to comply. The Banking Code Standards Board provides a list of financial institutions which follow the Code.

[132] Regulation 21of the DSRs. Similar protections exist under the Consumer Credit Act.

[133] Get Safe Online (2006a).

[134] www.apacs.org.uk/media_centre/press/22.09.06.html.

[135] See GSOL website: www.getsafeonline.org.

[136] Get Safe Online (2006a).

[137] AOL (2004).

4.42. APACs research also shows that despite the increased publicity that phishing has received, the number of people who would follow a link in an email purporting to be from their bank has not fallen significantly since 2004, when the issue first came to prominence (4 per cent of people in 2004, 3.8 per cent in 2006).[138]

4.43. When it comes to shopping online, consumers need to check for key signals that a site is secure. However, although 46 per cent of internet users told us that they always check the security of a site, 34 per cent only do so sometimes and one in five (19 per cent) never check. One reason appeared to be apathy among those who only sometimes or never checked: 28 per cent said that they 'just don't bother'.

4.44. Furthermore, our survey found that a large number of respondents were unable to recognise standard indicators that a website is secure:

- Only 32 per cent recognised that 'https' indicated a secure site
- Forty-two per cent of people did not know that clicking on the padlock symbol would let them see the certificates. Furthermore, many focus group participants knew about the security padlock symbol but did not know what it meant.

4.45. Worryingly, significant numbers of people relied on inaccurate measures of security:

- Sixty-one per cent of consumers felt that having to enter a password indicated that a site was secure
- Twenty-seven per cent relied on the fact that the site 'looked' secure.

## To what extent are businesses using technical protections?

4.46. In our business survey, 38 per cent of businesses were not taking payments online at all, or were taking card details online using a secure order form, and then processing payments offline. While online payment may not suit the needs of every kind of business, worries about the security of payments and associated e-crime were the largest reason (33 per cent) why businesses sold, but did not complete transactions, online. However, initiatives such as SSL, 3DSecure, and PCI DSS, have collectively provided a protective framework which heightens security. The promoters of these initiatives argue that businesses which implement these measures can take payments online with confidence.

4.47. With this in mind, we considered available evidence for the extent to which some of the technical protections were being used by businesses:

- **Secure socket layer (SSL):** PWC reported in 2003 that 89 per cent of UK e-commerce websites were protected with SSL, the highest rate of any country in their survey (EU15).[139] Our own survey found almost all sites provided evidence that they were using secure links (such as https or the padlock symbol). Indeed, 68 per cent of electrical and 67 per cent of travel sites showed use of secure links at all points where consumers were asked for information, although only 18 per cent of music sites did so.

  However, 30 per cent of electrical sites, 31 per cent of travel sites and 74 per cent of music sites only showed use of secure links when card details were requested. Furthermore, a small proportion of sites did not appear to use secure links when

[138] www.apacs.org.uk/media_centre/press/22.09.06.html

[139] PWC (2003) p.141.

collecting card details: 2 per cent of electrical sites, 6 per cent of travel sites and 8 per cent of music sites. It is of concern that some sites still do not appear to provide secure connections when collecting such important information.

- **PCI DSS:** Among the EU15, the UK has the highest proportion, 36 per cent, of e-commerce websites that store credit card information. In addition 99 per cent store names and addresses of customers.[140] Given this, it is particularly important that UK businesses maintain high standards of data storage. PCI DSS is a response to this need for high standards. There is little public information to shed light on data storage standards, but a 2006 survey by the Logic Group[141] found that only three per cent of merchants were PCI DSS compliant. While 71 per cent felt that they would be compliant within 18 months,[142] 16 per cent had no plans to implement the standard in the near future.
- **3D-Secure:** In our survey, 42 per cent of businesses said that lower fraud risks would make them more likely to sell or take payments online. The proponents of 3-D Secure consider that it provides a mechanism to lower this risk, and thus liability for fraud. Although we have no consolidated data on the take up of 3-D Secure, one source recently reported that 49 per cent of retailers were using it in 2006.[143] VISA recently indicated that by October 2006 more than 12,000 UK retailers and three million cardholders were enrolled for Verified by Visa and approximately one in eight Visa transactions was authenticated by 3-D Secure.[144] The stakeholders we consulted were confident that a critical mass would be reached in 2007.
- **CVC and AVS:** Cybersource's 2007 Online Fraud Report reports that Card Verification Code is the most common means of fraud prevention, used by 79 per cent of merchants. The Address Verification Service is used by 71 per cent.[145]

4.48. It seems that the industry is responding to consumers' and businesses' security concerns, by developing technical protections that seek to counter evolving threats. While we have not assessed the effectiveness of these initiatives, however, the extent of consumer concerns means that traders need to consider very carefully all the means available to them to provide cost-effectively a safe and reliable environment, and to communicate clearly to users how they are doing so. At the very least, they should be using secure connections when requesting customers' details.

## Sources of advice

4.49. In recent years, the media have often carried articles with advice on threat avoidance. Some larger ISPs offer security advice either online or via an advice line; provide their consumers with security products free of charge or at reduced cost; and offer a range of links to sites that sell security products. Furthermore, numerous websites provide guidance to businesses and consumers (see Box 4.3).

[140] PWC (2003).

[141] www.the-logic-group.com/Press/prerel_pci_survey_results.htm.

[142] The deadline to comply is 30th June 2007, after which organisations in breach could be fined.

[143] CyberSource (2007), p.9.

[144] Visa (2006).

[145] CyberSource (2007).

### Box 4.3: Some examples of websites offering advice on security

- Get Safe On Line – www.getsafeonline.org
- Crimestoppers – www.crimestoppers-uk.org
- Fraud Reduction – www.uk-fraud.info
- Home Office Website – www.homeoffice.gov.uk
- Metropolitan Police Fraud Alert – www.met.police.uk/fraudalert
- General identity fraud/theft information – www.identityfraud.org.uk
- APACS – the UK payments association – www.apacs.org.uk
- Bank Safe Online – www.banksafeonline.org.uk
- British Bankers' Association – www.bba.org.uk
- CardWatch – www.cardwatch.org.uk
- CIFAS – www.cifas.org.uk
- ITSafe – www.itsafe.gov.uk
- Business Link – www.businesslink.gov.uk
- OFT – www.oft.gov.uk
- Consumer Direct – www.consumerdirect.gov.uk

4.50. Get Safe Online (GSOL), in particular is an important development – a national campaign launched in 2005 to educate UK businesses and consumers in security and privacy issues.[146]

4.51. GSOL's 2006 survey found some improvement in security awareness following the launch of its campaign, but despite this, 72 per cent of respondents said they needed further information about online safety and 40 per cent of consumers are still not sure where to get internet safety advice. Furthermore, they found 35 per cent of respondents would turn to friends and family for advice, compared to only 25 per cent who would use an internet safety website.[147]

4.52. Overall, consumer awareness of the protections that exist remains disappointing given the high profile of the threats and the range of potential sources of advice available. With this in mind, many businesses and trade bodies considered that there would be value in having one central dedicated website updating consumers and businesses on all the technical, regulatory and all the other key information needed for successful online shopping.

[146] The GSOL campaign was launched as a joint initiative between HM Government, the police and private sector sponsors in October 2005, to raise awareness of the issues and provide solutions through a new website: www.getsafeonline.org and roadshows.

[147] Get Safe Online (2006a).

### The tone of advice

4.53. Furthermore, while it is encouraging that so many organisations wish to advise consumers, some of those we spoke to told us that the nature of some campaigns might raise fears unnecessarily. Although some organisations also told us that there could be benefits in 'scaring' internet users to secure their attention and encourage action, this could be leaving some less confident rather than more secure. There is some evidence of this: GSOL found that 24 per cent of survey respondents felt more secure through increased knowledge, but 19 per cent felt less secure once they were aware of the risks. This suggests a need for careful balancing in the messages given to shoppers.

4.54. Similarly, our survey of internet users who had concerns about shopping online found that 39 per cent cited the advertising of security products as one reason for their fears. While this was not an issue we explored in depth, it does underline the need for consumers to bear in mind that advertisers may not necessarily be presenting a balanced picture of the risks when selling products.

## Conclusions

4.55. Consumers and businesses most fear risks to payment security and privacy from e-commerce, but most stakeholders considered their concerns were disproportionate. Some of the dangers commonly associated with internet shopping may be more a result of data lost offline or through general internet usage, rather than the result of having shopped online.

4.56. Nevertheless, there are risks attached to using the internet, and to selling and shopping online, which need to be taken seriously. To guard against risks to their businesses and to address consumers' concerns (which put some off shopping online altogether), it is in traders' best interests to consider the range of technical and other protective measures they can take. Likewise, online shoppers can reduce risks by taking precautions and watching for warning signs. However, public awareness of these precautions and protections remains weak, despite campaigns and numerous sources of advice.

4.57. Awareness campaigns, as well as commercial advertising may also be scaring people away from shopping online as much as they are informing them. Some level of concern may helpfully encourage people to be vigilant, but campaigns need to be balanced, so that shoppers know how to protect themselves, without having excessive fears about online shopping. Consumers also need to bear in mind that advertisers may not necessarily be presenting a balanced picture of the risks when selling products.

### Next steps

4.58. We want to work with interested parties in this field to encourage the development and provision of more accurate ways of assessing the risks of online shopping. We also want to work with them to ensure that shoppers have an accurate view of the risks and know how to protect themselves, and that businesses are encouraged to provide a safe shopping environment. We also want to raise awareness of what shoppers can do if something goes wrong.

# 5 PROBLEMS AND REDRESS

## Summary

While consumers may primarily be concerned about security and privacy, where they actually experience problems, these are mainly of a conventional nature associated with distance selling.

We asked internet shoppers if they had experienced any problems when shopping online. Nearly a quarter (23 per cent) told us that they had experienced at least one problem when buying online in the previous year. It was difficult accurately to compare their responses with the experience of shopping though other channels, but our data on complaints suggests that the volume of consumer complaints does not appear unusual when compared to other distance selling channels, and that the types of complaints match those for mail order.

We found that most consumers complained when they experienced a problem – mostly to the retailer – and that they usually secured redress. However, one in five (20 per cent) had given up trying to resolve the problem. We also found that older and less experienced shoppers were least likely to have complained and most likely to have given up trying to resolve the problem.

Shoppers and online traders told us that delivery was where most problems cropped up: indeed it accounted for nearly half (48 per cent) of all the problems people said they had experienced (usually due to late or non-delivery). The annual economic detriment from unresolved delivery problems for online sales could be as much as £25 million to £55 million per year, excluding time and effort spent on successfully resolved problems.

Better communication between the main parties involved in delivery could be key to addressing some of problems experienced. Royal Mail and businesses told us of measures being put in place to meet the rapidly increasing demand for delivery services resulting from the growth of internet shopping.

## Next steps

In later chapters we consider the importance of raising consumer and business awareness of their respective rights and obligations. We will consider whether this could include raising awareness of how to prevent the most typical problems, like difficulties with delivery, as well as to ensure businesses know not to impose insurance conditions on shoppers.

## Introduction

5.1. While the last Chapter considered issues that affect consumer confidence in relation to security and privacy concerns, this Chapter considers consumers' less pronounced concerns relating to the more traditional problems raised by distance selling. Every year, consumers make many millions of purchases online without any problems. However in a minority of cases, they do experience difficulties.

## Online shoppers' experiences of problems

5.2. Although shoppers told us that they were most concerned about perceived security and privacy risks from online shopping, worries about some of the more conventional problems associated with distance shopping were also an issue. Twenty-three per cent were concerned about late or non-delivery of their purchases, and 16 per cent cited concerns about product quality.

5.3. In focus groups, consumers told us that getting the wrong product was a risk they associated with internet shopping and linked to this, unawareness about what to do in this situation. The majority of internet shoppers indicated that they did not know where or how they would send items back to the seller if this was required, whether the postage would be paid, and how long they would have to return the item.

5.4. In this Chapter, we consider what problems consumers have actually experienced, while in the next Chapter we address what rights they have to deal with these problems.

### What problems do online shoppers experience?

5.5. Our consumer survey found that 23 per cent of internet shoppers had experienced some form of problem in an online transaction in the last year, which we estimate means at least one problem experienced for every 58 transactions.[148]

5.6. Where consumers claimed to have experienced a problem, the value of the goods involved was fairly modest. In 45 per cent of cases they were worth £40 or less; and in 67 per cent the value was below £100. The median value of the products for which consumers had experienced their most recent problem was around £46, which was very similar to market research figures on the average purchase online: £42 in 2005.[149]

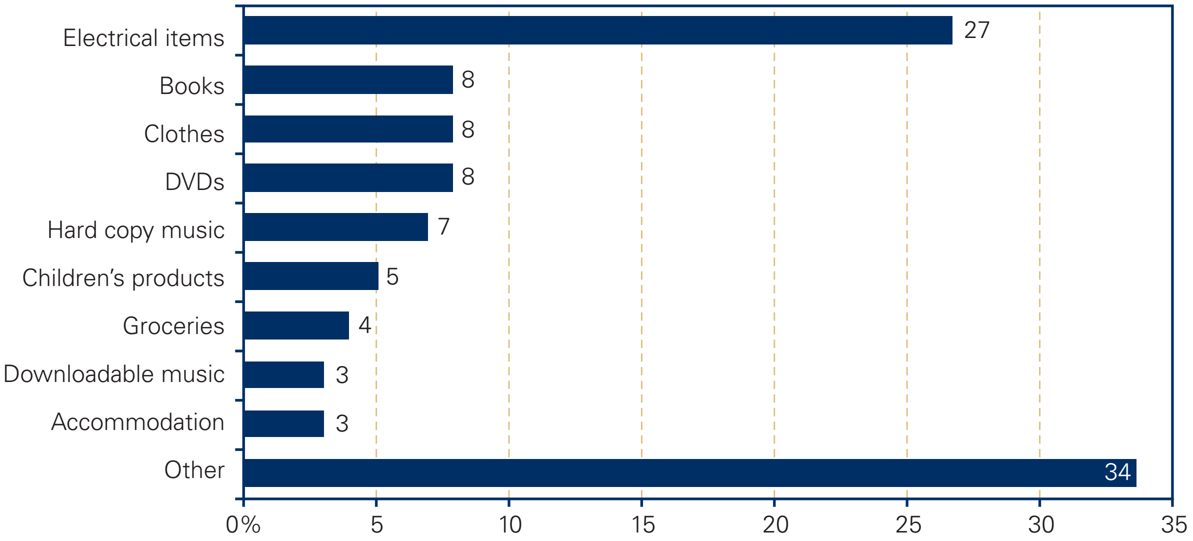
5.7. A wide range of items were being bought when problems were encountered (see chart 5.1). The main product type involved was electrical items with over one in four (27 per cent) of the problems most recently experienced having occurred when buying this type of product. However, this may reflect the high proportion of all internet transactions which are for electrical goods as well as the nature of electrical items which might be more complex and fragile than many other products purchased online.

5.8. For internet shoppers who told us that they had encountered a problem, most (69 per cent) said that the most recent problem had been encountered when buying from a retailer that they believed did not have a high street presence, while 27 per cent said that the business also sold on the high street.

[148] While our survey found that 23 per cent of internet shoppers had experienced a problem in the twelve months to November 2006, we cannot tell whether they experienced more than one problem per single purchase or multiple problems (in other words, problems with more than one of the products they purchased). However, if we make a conservative assumption that they experienced one problem with one purchase during the year and assume that on average internet shoppers made 13.2 purchases over the internet (Verdict, 2005), this suggests that consumers encountered some form of problem for 1.7 per cent of purchases (or one for every 58 transactions). We cannot compare this to other retail channels because of the difficulty in obtaining reliable data on numbers of transactions and numbers of problems.

[149] Source: Verdict 2005.

## Chart 5.1: The last item bought for which consumers experienced a problem (%)



Source: OFT Consumer telephone survey

Base: All internet shoppers who have encountered a problem within the last 12 months and non-shoppers who have had a bad experience online shopping previously

### How does online shopping compare?

5.9. It is very hard to compare experiences across different retail channels.[150] However, businesses we met and in our survey claimed no greater level of complaints for online compared to traditional sales channels. Of those businesses able to compare on/offline complaints, four in five (78 per cent) said that online complaints were the same or lower than offline.

5.10. Most online businesses who commented disputed that consumers were more likely to experience problems when buying online from legitimate businesses. They argued that online shoppers benefited from more information; greater hands-on control of the purchase process (including order tracking in some cases); and the benefit of a cancellation period.

5.11. Complaints data from Consumer Direct, the national telephone and online consumer advice service[151], suggests that the volume of consumer complaints does not appear unusual when compared to other distance selling channels (Table 5.1), although care must be taken when interpreting these figures.[152] However, as might be expected, the proportion of complaints relating to internet purchases has been rising (from 4.6 per cent in the third quarter of 2004 to 7.9 per cent in 2006), in line with the increase in sales to households. If such growth continues, the internet may in a few years overtake telephone sales to become the second main source of complaints to Consumer Direct in terms of retail channel.

[150] Reliable comparisons would require data on the level of complaints, the number of purchases and the problems consumers have experienced in each sales channel. This would rely on consumer recall and would require them to remember the details accurately. Comparisons are further hindered by the different nature of the channels themselves making some types of problem more likely for one than another. Comparisons with offline sales are particularly difficult given the often large number of daily purchases for a typical consumer.

[151] Consumer Direct aims to give consumers clear, practical and impartial advice to help them resolve problems or disagreements with suppliers. The OFT has managed Consumer Direct since April 2006. See: www.consumerdirect.gov.uk

[152] The purchase method (internet, high street, etc), the nature of the trader or of the problem was not always clear from the historic data available to us, although work is underway to enhance the quality of data recording. And some cases may be enquiries rather than complaints. It is important to note that complaints data may not represent the experiences of consumers more generally.

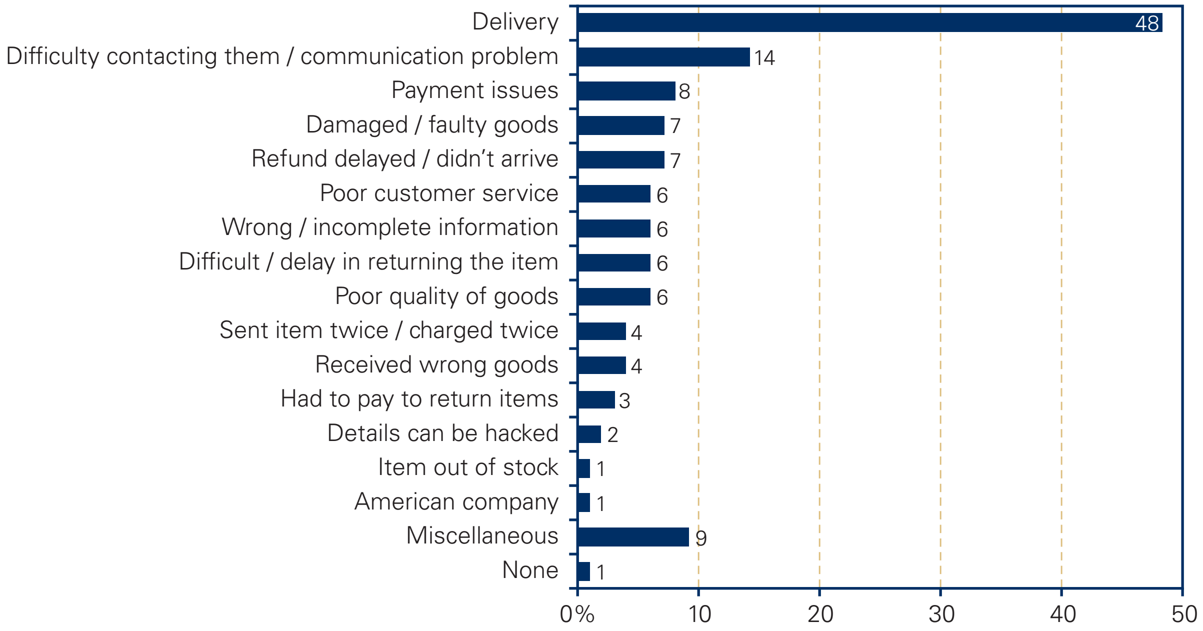
### Table 5.1: Consumer complaints by purchase mode (2006)

| Purchase mode | % of all complaints to Consumer Direct where purchase mode is known |
|---|---|
| Trader premises | 58.1 |
| Telephone | 9.1 |
| Internet[153] | 7.9 |
| Doorstep invited | 5.9 |
| Unsolicited postal | 2.9 |
| Mail order | 2.3 |

Source: Consumer Direct

5.12. Evidence from our surveys and data on complaints to Consumer Direct also suggested that consumers experience the sorts of problems that might typically be expected when buying over a distance. In our survey, about half (48 per cent) of those who had experienced a problem shopping online in the past 12 months said the most recent problem related to delivery. The second most frequently mentioned problems related to problems communicating with the trader (14 per cent). However, when combined, wrong, damaged, faulty or poor quality goods were also a typical cause of complaint, accounting for 17 per cent of the problems most recently experienced. Likewise, when combined, difficulties with refunds and returns accounted for 16 per cent of problems consumers said they had experienced.

### Chart 5.2: What types of problems did online shoppers experience?



Source: OFT Consumer telephone survey

Base: All internet shoppers who have encountered a problem within the last 12 months and non-shoppers who have had a bad experience online shopping previously

[153] Excluding internet auctions. If these are included, the figure is 8.4 per cent.

5.13. The types of complaints recorded by Consumer Direct for internet-related purchases were also similar to other distance selling channels – especially those for mail order (see Table 5.2). Although 'defective goods' was the main problem recorded for complaints relating to internet purchases, this was also true of most means of buying. However, problems relating to the distance between buyer and seller (delivery, collection and repair) were considerably higher than for purchases from trader premises.

**Table 5.2: Top 5 types of complaints recorded (2006)[154]**

| Complaint | Trader premises | Telephone | Mail order | Internet |
|---|---|---|---|---|
| Defective goods | 54% | 28% | 37% | 38% |
| Delivery / Collection / Repair | 5% | 10% | 25% | 23% |
| Misleading claims / Omissions | 7% | 9% | 8% | 11% |
| Substandard services | 21% | 32% | 12% | 14% |
| Prices | 3% | 5% | 3% | 3% |

Source: Consumer Direct

5.14. Businesses told us that a significantly higher proportion of problems with online sales than offline sales related to delivery. When businesses were asked what the complaints they received regarding online sales most commonly concerned, 18 per cent replied 'non-delivery of goods', eight per cent 'delivery of wrong goods', and seven per cent 'delivery times/slow/delayed'. The corresponding figures for offline sales were five per cent, three per cent and two per cent respectively.

5.15. Delivery also featured as a key issue in our focus groups. Either shoppers considered the wait for goods was too long, or there was a lack of information about how long delivery would take. Having to be at home and take time off work to wait in for a delivery was also a strong barrier to purchasing online. Security was a key concern for those needing a delivery to an address where no one would be in. This was particularly so for residents in flats who feared theft from their doorstep. Participants described stories of courier companies leaving goods outside the door, or in an insecure place (dustbin / recycle box):

*'I've had stuff stolen from outside my door… that's the problem when you live in a block of flats'.* (Internet shopper, Croydon, younger)

## How online shoppers act when they encounter a problem

5.16. Although nearly three quarters (72 per cent) of internet users thought that problems were harder to resolve when shopping online than on the high street, most (63 per cent) online shoppers who had experienced a problem in the past 12 months, had had it resolved to their satisfaction.

5.17. The majority (79 per cent) of online shoppers who had experienced problems had complained: 61 per cent of those with problems had complained to the seller, with smaller numbers complaining to others, including Consumer Direct (five per cent). Two-thirds (65 per cent) of those who complained to the seller achieved a satisfactory resolution, suggesting that this should be the first port of call for discontented consumers.[155]

[154] Percentage of complaints relating to purchase method (for instance, 54 per cent of all complaints transacted on trader premises related to defective goods).

[155] The numbers are too small for robust conclusions on the effectiveness of complaints to other organisations.

5.18. However, one in five (20 per cent) of those who experienced a problem had given up trying to resolve the problem, and 17 per cent were still trying to achieve redress.

## Delivery

5.19. Focusing on delivery, since this was by far the most commonly cited problem, it is encouraging that 63 per cent of internet shoppers who had experienced delivery problems felt that the problem had been resolved to their satisfaction. Some of the delivery resolutions may reflect instances where the delivery was simply late, but ultimately turned up.

5.20. Some businesses suggested that delivery problems partly represented the market entry of traders with less experience of inventory management and the logistics of home deliveries, and that these problems would therefore gradually be ironed out, especially with greater use of order tracking.

5.21. Nevertheless, given the volume of transactions and because it is the most significant problem, unresolved delivery remains a substantial issue. If we assume that all those internet shoppers who had an unresolved problem with online delivery in the last year suffered detriment of between £55 and £115 based on the mean value of the item involved in these types of problems,[156] aggregate annual detriment could be as much as £25 million to £55 million per year. This includes unresolved problems only, whatever they might have been, and neglects time and effort spent on successfully resolved problems.

5.22. In terms of the security worries voiced by shoppers about left packages, there is some evidence that consumers themselves may need to do more to avoid taking unnecessary risks. Recent research found that over 13 per cent of consumers were prepared for deliveries to be left on their doorstep, the second year running the proportion had increased.[157] Some of the bigger players also told us that they were no longer displaying their brand names on parcels, or were now recording the weights of all packages to address the potential for theft throughout the delivery process.

5.23. Furthermore, recent research for Royal Mail found that fewer consumers were having home shopping delivered to their own homes (92 per cent of home shoppers in 2006, down from 97 per cent in 2004) with more having deliveries sent to locations such as neighbours' houses (29 per cent), Royal Mail sorting offices (17 per cent) or work (11 per cent).[158]

5.24. Successful delivery requires at least three parties – the seller, courier and recipient – to communicate effectively with one another to ensure there is full understanding of item type, address and time for delivery. Many stakeholders suggested that this three-way communication was critical. Some businesses emphasised the importance of tight contractual obligations with delivery companies. Others said it would be helped by early agreement of precise delivery windows. Research by Royal Mail[159] has found that being able to specify delivery day and time are the most important requirements for consumers; with younger age groups, in particular wanting to be able to specify time of day, as well as the day.

[156] We assumed that the upper limit of consumer detriment with regards to an unresolved problem was the total value of the product bought. While this assumed that the consumer did not receive the product at all, it was still a cautious approach, because further costs involved in trying to resolve the problem and emotional issues were not included. The lower limit was assumed to be 50 per cent of the value of the product in question, assuming that this represents some time spent or other costs to consumers in attempting to resolve the problem even if they received redress.

[157] Verdict (2006).

[158] Royal Mail (2006).

[159] Royal Mail (2004).

5.25. On the other hand, some businesses felt that consumers may have unrealistic expectations. Home deliveries could fail for many reasons, including misunderstandings between the parties; non attendance by consumers; packages left with third parties and not passed on; vehicle breakdowns and unpredictable traffic.

5.26. It is normal practice for retailers to take full responsibility for safe product delivery when dealing with consumers.[160] However, the parties may have different understandings as to what amounts to delivery. It is important, therefore, that consumers and retailers seek to agree when, and how, delivery will take place to avoid misunderstandings and possible disputes.

5.27. Effective communication between the key parties is crucial to preventing delivery problems, and businesses told us that the internet retailing industry as a whole had worked together in recent years to improve delivery for consumers. Increasingly, for example, retailers were allowing people to have items delivered to an address other than their home address, and offering a range of delivery speeds. Other retailers who mainly sold online were also offering pick up points.

5.28. Royal Mail also told us that their measures to meet the rapidly increasing demand for effective delivery services included a Local Collect service, which allows people not at home when delivery is attempted to ask for items to be taken to their local Post Office branch. More recently (June 2007) Royal Mail launched a service allowing consumers to designate a safe place on their premises, for example a garden shed, where a delivery can be left if they are not at home. The customer does this at the point of ordering goods with registered retailers who offer the service.

5.29. Finally, it was also suggested to us that some retailers may include a standard term on their website which requires buyers to pay insurance to cover the risk of damage to the product during delivery. If the purchaser is a consumer, the goods remain at the seller's risk until delivered, and so there is no reason for a buyer to take out such insurance. Inclusion of such a term, or any term suggesting that goods are at the consumers risk prior to delivery, is likely to be an unfair contract term under the Unfair Contract Terms in Consumer Contracts Regulations 1999, as it seeks to reduce the rights of a consumer if the retailer fails to achieve a satisfactory delivery of the product.

5.30. Although we heard anecdotal evidence for the practice of adding compulsory insurance, our review did not find it to feature much on the sites examined (although this may in part reflect our choice of case studies). Only one electrical retailer appeared to include a standard term on their website requiring the consumer to pay insurance to cover the risk of damage to the product during delivery. Nevertheless, it is important that businesses do not try to unfairly pass risk of damage or loss to consumers, and shoppers should be on the alert for this.

[160] Under section 20(4) of the Sale of Goods Act 1979, in a case where the buyer deals as a consumer, the goods remain at the seller's risk until they are delivered to the consumer.

## Conclusions

5.31. While consumers may primarily be concerned about security and privacy, they mainly experience conventional problems associated with distance selling. It was difficult accurately to compare their responses with the experience of shopping through other channels, but our data on complaints suggests that the volume of consumer complaints does not appear unusual when compared to other distance selling channels, and that the types of complaints match those for mail order.

5.32. The most significant issue is delivery, which accounts for nearly half (48 per cent) of all problems. Here, effective communication seems to be the key requirement to preventing problems. However, other issues included problems with the items themselves, with returns and refunds and with contacting the traders concerned. We explore in the next chapter the relevant regulatory protections for consumers buying at a distance.

### Next steps

5.33. In later chapters we consider the importance of raising consumer and business awareness of their respective rights and obligations. We will consider whether this could include raising awareness of how to prevent the most typical problems, like difficulties with delivery, as well as to ensure businesses know not to impose insurance conditions on shoppers.

# 6 CONSUMER RIGHTS: AWARENESS AND COMPLIANCE

## Summary

We focused on the regulations with particular relevance to the distance selling nature of internet shopping. Although these appear broadly fit for purpose at present, we identified a number of areas where they could need updating to take account of new developments such as mobile commerce and downloads. Because the laws derive from Europe, we have brought these to the attention of the European Commission, who are currently reviewing how they might need to be changed.

However, although the regulations may not be problematic, awareness of them seems weak. For instance, shoppers need to know, when they buy, that they have the right to cancel, so that they do not unnecessarily keep products that on examination they do not want. However, we found that more than half (56 per cent) of the internet shoppers we surveyed online did not know about their right to cancel, and many (29 per cent) also did not know where to turn to get advice on their rights.

We also found that a lot of traders had a weak awareness of the law themselves. For example, in our survey of UK-based online traders, 28 per cent said that they were not aware or only slightly aware of the laws applying to internet shopping, and two-thirds (66 per cent) had never sought advice on them. One fifth of online electrical retailers did not think that buyers had a right to cancel, and more than half wrongly thought that they could withhold the cost of outward delivery when refunding shoppers.

When we looked at websites, we found that one in ten (12 per cent) of electrical sites and nearly four in ten (39 per cent) of music retailers' sites selling CDs did not appear to mention the cancellation period. Furthermore, there was evidence that some sites might be trying to impose conditions that could prevent or at least deter consumers from exercising their cancellation rights. For instance, 59 per cent of electrical sites stated at least one condition on consumers' rights to cancel and receive a refund which may have led to a breach of the regulations.

Businesses told us that guidance on the key legal requirements should be clearer and have a higher profile. While many different sources of advice are currently available, each tends to address separate issues, for example general consumer rights, distance selling obligations, the law on privacy, guidance about online threats and safety. Many organisations said that they would welcome a single dedicated, clear source or signpost, to cover all the information needs for internet sellers and shoppers.

## Next steps

We will develop and implement a strategy employing the most effective and innovative ways actively to raise business and consumer awareness of online shoppers' rights – both directly and by working with third parties. We will also look into whether and how the wider range of relevant advice to internet traders and buyers could be more co-ordinated. We will encourage industry to self-assess, to make sure it is complying with the relevant legislation. Enforcement may ultimately be considered, to target outstanding breaches that create clear detriment.

## Introduction

6.1. This Chapter outlines the regulatory protections available to consumers shopping on the internet, focusing in particular on the additional rights relating to the distance between buyer and seller in online transactions, and the nature of the medium used, and considers the extent to which the protections are relevant and adapting, as well as whether businesses and consumers know of them.

## Regulations with specific relevance to internet shopping[161]

6.2. Anyone buying online from a UK-based business has at least the same rights as if they were buying on the High Street (and similar rights when purchasing from other Member States). However, people shopping at a distance cannot physically examine what they are buying and may have no direct contact with the seller.

6.3. As well as the full raft of general consumer protection legislation, and that addressing specific concerns, such as privacy and security, the regulatory framework includes two sets of regulations of particular relevance to internet shopping:

- Consumer Protection (Distance Selling) Regulations 2000 ('DSRs')
- The Electronic Commerce (EC Directive) Regulations 2002 ('ECRs')

### The Distance Selling Regulations (DSRs)

6.4. The DSRs implement the EC Directive on Distance Selling, the purpose of which was to encourage cross border trade by giving consumers the confidence to buy over the internet, by mail order or the phone by giving them additional consumer rights.[162]

6.5. Broadly speaking the DSRs apply to contracts for goods and services supplied to consumers where they have no face to face contact with the supplier – for instance by mail order, the phone, fax or interactive TV. They also apply to buying on the internet. At the heart of the DSRs is the provision of information to enable consumers to make informed buying decisions, and a right for them to cancel most contracts within a certain period. Box 6.1 outlines the main elements.

**Box 6.1: Consumer rights under the DSRs**

If you are buying at a distance – including over the internet – the business must provide you with key information, including:

- its legal identity
- if payment is required in advance, its geographic address
- a description of the main characteristics of the goods or services
- the price of the goods or services, including all taxes
- details of any delivery costs where appropriate
- details of how payment can be made
- the arrangements for delivery or performance of the service
- your right to cancel (unless the contract is for goods and services which are excepted from this)

[161] This section is not intended to provide a complete statement of the law. The OFT has also issued 'A Guide for Businesses on Distance Selling', which is available at www.oft.gov.uk/shared_oft/business_leaflets/general/oft698.pdf. There are many other sources of guidance available – including advice for consumers on the OFT and Consumer Direct websites. Chapter 8 also discusses some specific guidance that has been issued.

[162] The Regulatory Impact Assessment (RIA) for the Distance Selling Regulations states its objective: *'…The regulations will provide statutory rights that counterbalance the fact that they do not have the opportunity to inspect the quality and suitability of goods and services before placing an order to buy them. They will also help to strengthen consumer confidence in the use of new media and in cross-border shopping in the EU…'*. See: www.dti.gov.uk/files/file35725.pdf,

Once you decide to buy, the trader has to provide you in writing (or another 'durable medium') the information listed above together with information about the conditions and procedures for exercising your right to cancel.[163] They must also tell you the address to which you can address any complaints.

You also have the right to:

- cancel the contract within a short period, usually seven working days.
- a refund of the cost of the goods or services together with all sums paid in relation to the contract (such as delivery costs) as soon as possible after cancellation and in any case within 30 days at the latest
- delivery of the goods, or performance of the service by the trader, within 30 days from the day after the day you send the order to the business (or other period as agreed)
- protection from the fraudulent use of your payment card

6.6. Where they do apply, any term in a contract which is inconsistent with the DSRs is void. There are some exceptions though and some contracts to which only part of the DSRs apply. For example, the DSRs do not apply to:

- Business to Business (B2B) sales
- the sale of land, or financial services (which are covered by other regulations)
- sales concluded at an auction
- where a business only occasionally sells by distance means.

6.7. They also only partially apply in some cases. For instance:

- the information requirements, the right to cancel and the requirement to carry out the contract within 30 days do not apply to the supply of food, drinks, or goods by regular roundsmen (such as milkmen), accommodation and transport, catering or leisure services
- specific requirements concerning the carrying out of the contract do not apply to timeshare agreements and package travel.

## The Electronic Commerce Regulations (ECRs)

6.8. The ECRs also implement an EC Directive, and apply to businesses which sell or advertise goods or services to consumers (and to other businesses) on the internet.[164] They provide buyers with the right to certain general information in a form which is easily, directly and permanently available (see Box 6.2).

[163] The time limits for cancellation of contracts for goods and services depend on when the consumer receives the required written information.

[164] The ECRs govern the provision of Information Society Services, a term that covers any service normally provided for payment, at a distance, by means of electronic equipment at the individual request of a recipient of a service. The goods and/or services do not have to be provided electronically for the ECRs to apply. The ECRs do not apply to online activities which are not of a commercial nature, to the goods themselves, or the delivery of the goods or services not provided online or to the offline elements (such as the conclusion of a hardcopy contract) of any transaction that began online (such as in response to an advert on a website).

### Box 6.2: The ECRs and online shopping

If you are buying from a business selling or advertising on the internet, the business must give you certain information, including the following:

- Full name of the business
- Geographic address where it is established
- The trader's contact details including an email address to enable you to contact the trader rapidly and effectively
- The trader's VAT number if they are subject to VAT
- Where a business refers to the price of goods and/or services, a clear and unambiguous indication of those prices and, in particular, whether the prices include taxes and delivery costs.

If the contract is made entirely online, which may typically be the case if you order on a website the business must also give you the following information in a clear, comprehensible and unambiguous manner:

- the different technical steps to follow to conclude the contract
- whether or not the contract will be filed by the trader and whether it will be accessible to you
- how you can identify and correct input errors prior to placing the order
- any relevant codes of conduct which the trader subscribes to and information as to how they may be consulted electronically
- where a business provides terms and conditions that are applicable to the contract they must be made available in a way that allows you to store and reproduce them

You also have the following rights:

- Where you place an order through technological means, you must receive acknowledgement of receipt of the order electronically without undue delay.
- You must also be able clearly to identify if an email is advertising and which trader has sent it.[165]

## Other key legislation

6.9. UK consumers shopping online from a UK-based business are entitled to all the rights they have if they are shopping from the High Street. There are many regulations protecting consumers, with which businesses need to comply. Some key examples include:

[165] The Privacy and Electronic Communications (EC Directive) Regulations 2003 set out the rules which apply to unsolicited direct marketing messages sent by a range of methods, including emails. See Chapter 3.

Table 6.1: Brief description of other key legislation applicable to internet shopping

| Legislation | Summary |
|---|---|
| **Trade Descriptions Act 1968 ('TDA')** | This requires a trader to ensure any descriptions applied to goods and services they supply or offer to supply are accurate. |
| **Consumer Credit Act 1974 ('CCA')** | This regulates consumer credit activities including what is required in documentation, advertising, and the calculation of the cost of credit. Section 75 provides a consumer with additional protection if they use their credit card (or certain other credit agreements) to pay for goods or services between the value of £100 and £30,000. See discussion and Box 6.3 below. |
| **Unfair Contract Terms Act 1977 ('UCTA')** | Under this Act certain contract terms, and other notices excluding or restricting liability are made unenforceable, while others are subject to a reasonableness test. Attempting to impose void terms on consumers may be illegal under the Consumer Transactions (Restrictions on Statements) Order 1976. |
| **Sale of Goods Act 1979 ('SGA')** | This provides (amongst other things) that when a trader sells goods to a consumer, the consumer can take action if they are not as described or not of satisfactory quality. It also sets out the remedies available to consumers. |
| **Supply of Goods and Services Act 1982 ('SGS')** | This gives consumers the right to expect that a supplier of a service acting in the course of a business will carry out that service with reasonable care and skill and, unless agreed otherwise, within a reasonable time and for a reasonable charge. |
| **The Consumer Protection Act 1987 (Part III) ('CPA')** | This covers product safety and liability, and prohibits misleading price indications. |
| **Control of Misleading Advertisements Regulations 1988 ('CMARs')** | These provide protection against misleading advertisements and also set out requirements for advertisements that make comparisons with competitors. |
| **Data Protection Act 1998 ('DPA')** | The Data Protection Act provides a framework to ensure that personal information is handled properly. Businesses which process personal information must comply with eight principles. |
| **Unfair Terms in Consumer Contract Regulations 1999 ('UTCCRs')** | These require that standard terms used in contracts with consumers are clear and fair. |
| **Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECRs')** | The PECRs regulate unsolicited direct marketing messages sent by a range of methods including emails. |
| **Package Travel, Package Holiday and Package Tours Regulations 1992** | Regulates the sale of 'package holidays' – including the provision of of information, insolvency protection and liability in the event of problems. |

6.10. In the time available, we did not attempt to assess the effectiveness of the entire framework of regulations relevant to online shopping. We focused on the regulations with particular relevance to internet shopping – especially the DSRs. However, in this report, we do note some examples where other regulations have particular relevance:

**Table 6.2: Relevant regulations discussed in this report**

| Regulations | Discussed in... |
|---|---|
| • Privacy and Electronic Communications (EC Directive) Regulations 2003<br>• Data Protection Act 1998<br>• Consumer Credit Act 1974 | Chapters 3 and 4, in relation to unsolicited emails; and financial protections.<br>The CCA is also discussed in this Chapter. |
| • Unfair Terms in Consumer Contract Regulations 1999 | Chapter 5 in relation to deliveries |
| • The Consumer Protection Act 1987 (Part III)<br>• Control of Misleading Advertisements Regulations 1988 ('CMARs') | Chapter 9 in relation to the information presented on websites |
| • The Package Travel, Package Holidays and Package Tours Regulations 1992 | Chapter 10 in relation to the information presented on websites. |

6.11. Part III of the Consumer Protection Act 1987 (which deals with misleading prices), CMARs and a number of provisions in the Trade Descriptions Act 1968 will cease to have effect when the Consumer Protection from Unfair Trading Regulations, which implement the UCPD, are brought into force in 2008. The UCPD is considered in Chapter 12.

## Are the key regulations currently fit for purpose?

### Stakeholders' views on their effectiveness

6.12. A few businesses argued that, because the DSRs and Distance Selling Directive (DSD) were drafted in the early days of internet shopping, they did not accurately reflect the new balance of power the internet had brought. Their concern was that the wealth of information available to consumers on the internet had strengthened their position in relation to businesses, and that the regulations governing online sales should reflect this.

6.13. However, most businesses and other organisations who expressed a view said that the DSRs were generally effective.[166] Those we spoke to did not identify a need for significant changes. A few stated that they helped to boost consumer confidence. Furthermore, in our survey of businesses, 67 per cent said no parts of the law applying to internet shopping made selling online problematic (and 22 per cent did not know). Only 11 per cent thought that there were any problems with the law. Nor did the regulations appear to be a critical barrier to traders setting up online: only 23 per cent of businesses not trading online said changes to regulations would encourage them to do so – the least cited factor.

[166] However, it is possible that the low level of concern about the regulations could in part reflect apparently weak awareness of the regulations on the part of businesses (see later in this Chapter).

6.14. However, a few businesses expressed concerns about returns by consumers. They stated that the cancellation period was abused by some customers who used the products before returning them in an unfit condition for resale, or did not return products despite receiving refunds within the 30 day time-limit. Some businesses provided anecdotal evidence: one electricals retailer, for instance, cited a consumer who they felt had ordered a widescreen TV simply to watch the World Cup, before returning it for a refund.

6.15. We requested, but did not receive, any more detailed evidence from businesses who claimed this to be a problem. However, businesses' responses to our survey suggested that returns are rare. The majority (67 per cent) of businesses said that their level of non-faulty returns was less than one per cent of all their sales (and clearly not all of these returns would have been 'abusive').[167]

## Are the regulations keeping pace?

6.16. Some consumer groups and businesses thought that the DSRs might be getting out of date – particularly in the face of developments such as online auctions, mobile commerce and the convergence of platforms. However, the next few years represent a period of potentially significant change for the regulations because of reviews at the EC level.

6.17. The DSRs and the ECRs both derive from European law (the Distance Selling Directive and the Electronic Commerce Directive respectively). The Distance Selling Directive (DSD) is currently under review by the European Commission (EC), as part of a review of a raft of consumer protection Directives, known collectively as the 'consumer acquis'.[168] Given this review, changes are likely to occur to the DSRs at some point over the next few years. The second EC review of the Electronic Commerce Directive (ECD) is due later this year with a possible revision of the Directive likely to follow in 2008 – at the time of writing, it is unknown what implications this might have for the ECRs and internet shopping.

6.18. Drawing on our discussions with stakeholders and our own analysis, we submitted views to the Commission in November 2006 and May 2007 on what might be needed to harmonise and modernise the DSRs, as part of their wider consultation on the acquis. As well as supporting the development of common definitions across all the Directives of terms such as 'consumer' and 'supplier', we identified a number of areas where, looking ahead to new developments the Directive might need updating to protect consumers in the future. These included:

- The need to provide certain information 'in writing or another durable medium' may need to be revised in the light of new technologies. Some of the bodies we spoke to pointed to the difficulties of providing the requisite durable information in the context of potentially small screen displays, for example, on mobile phones.
- Uncertainty about how new types of information products are treated (downloaded software, music, etc). These are hard to categorise as either goods or services, which affects their legal status and their treatment under the regulations.[169]
- The fact that contracts concluded at an auction are exempt from the Distance Selling Directive, but that the Directive does not define an 'auction'. This has led to uncertainty as to whether people buying from businesses by bidding on online auction sites have a right to cancel. We discuss this issue further in Chapter 10.

[167] Twenty per cent did not respond. However, it is possible that the low level of returns could in part reflect apparently weak consumer awareness of their right to cancel (see later in this Chapter).

[168] The 'consumer acquis' comprises eight consumer protection Directives. The aim of the review is to modify, harmonise and clarify various consumer protection Directives. The Directives are being reviewed both as a whole and individually to identify gaps and shortcomings affecting all of them as well as problems specific to individual Directives like the DSD. See: Updating and simplifying the community acquis COM (2003) 71, European Contract Law and the revision of the acquis: the way forward COM (2004) 651 Final, Green Paper on the Review of the Consumer Acquis COM (2006) 744 final.

[169] The OFT considers these are likely to be services (paragraph 3.39 of 'A Guide for Businesses on Distance Selling', which is available at www.oft.gov.uk/shared_oft/business_leaflets/general/oft698.pdf.

## How aware are consumers of their rights?

6.19. Again, rather than test awareness of all the rights consumers have, we focused on those with specific relevance to someone buying online. Some of the businesses believed that consumers' willingness to complain demonstrated their awareness of their rights.

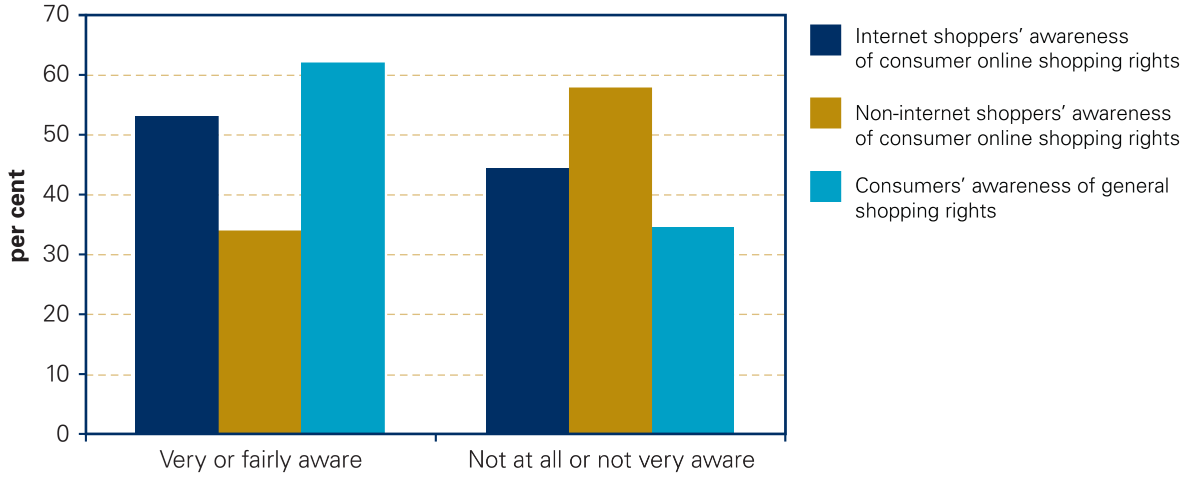
6.20. Some also felt that poor rights awareness might be inevitable, and that consumers were typically only interested in knowing their rights once something had gone wrong. However, the rights relating to distance selling are intended to raise confidence by ensuring buyers have key information *before* they make a purchase, including their right to cancel whether or not they have a problem with their purchase. In this sense, it is even more important that consumers know their rights.

### Consumer perceptions of their awareness

6.21. Most stakeholders, especially consumer bodies, believed consumer awareness of their rights generally when shopping was relatively low, and that awareness of their rights when shopping online was lower still.

6.22. Our surveys largely confirmed this. For instance, in the first quarter of 2006, 63 per cent of shoppers felt very or fairly well informed about their consumer rights generally. But when it came to awareness of what rights they have when buying online, only 54 per cent of internet shoppers felt very or fairly well informed, and only 34 per cent of non-internet shoppers felt similarly aware (see Chart 6.1).[170] These figures match those of other surveys.[171]

**Chart 6.1: Awareness of consumer rights**



Source: OFT Competition Act and Consumer Rights Research, March 2006 and TNS Omnibus conducted on behalf of OFT, January 2006

6.23. The results of our more recent telephone survey of consumers provided similar results: 56 per cent of internet shoppers claimed to be very or fairly aware of their rights. This suggested no substantial increase in awareness in the 10 months between the two surveys.

[170] Data on consumers' general awareness of rights is from the OFT Competition Act and Consumer Rights Research, March 2006. Data on internet shoppers' and non-internet shoppers' awareness of their rights when shopping online is from the TNS Omnibus conducted on behalf of OFT, January 2006.

[171] Forty per cent of people who have access to the internet feel that they do not know their consumer rights if shopping online. Richards (2005).

6.24. Many businesses also felt that consumers' awareness of their rights would grow with their experience of online shopping. There was some evidence to support a link between rights awareness and experience of online shopping (although we could not tell whether one caused the other). More experienced shoppers (regular shoppers and large spenders) claimed higher levels of awareness of their online shopping rights: 67 per cent claimed to be very or fairly aware compared to 46 per cent of less experienced shoppers.

6.25. Other OFT research[172] has also found variations among different groups of consumers in how confident they feel about using their rights when they need to make a complaint or return goods or services (purchased via any sales channel). While most (78 per cent) felt either very or fairly confident, this figure dropped to 59 per cent for the 16-18 age group, and to 65 per cent for over 75s.

6.26. Socio-economic factors also made a difference:[173] 74 per cent of those in the C2DE group felt confident in using their rights, compared to 82 per cent of ABC1s. Those who had completed further/higher education were also more confident than those who had not. And those in full-time employment were more confident than those not working.

## Consumers' actual awareness of their rights

6.27. When asked about their rights, consumers were actually less aware than they claimed to be. For instance, one of the most important rights for consumers shopping online is the seven-day cancellation period under the DSRs. However, when their knowledge was tested in our online survey, 56 per cent did not know of this cancellation period, or considered there was no such period.[174]

6.28. Other consumer surveys have similarly found weak actual awareness of online rights. In one, only 25 per cent of respondents said that online traders had legally to refund an item a consumer had bought but changed their mind about without there being anything wrong with the item.[175]

6.29. Consumers' knowledge of the cancellation period itself is also weak. In our telephone survey, 25 per cent of consumers who knew of the right to cancel thought that they had seven days to do so. A total of 63 per cent of respondents thought that they could cancel an order within 14 days. More than a quarter (27 per cent) thought the period was 28 days or more.

6.30. Again, however, there was some evidence that shoppers' knowledge of their rights might improve with experience of online shopping. For example, in our survey, when posed with a theoretical situation, 53 per cent of those who had shopped online for seven or more years correctly said that they had the right to cancel the order, compared to only 35 per cent of those who had shopped for one to two years. Similarly, a significantly higher proportion (48 per cent) of people who shopped online more than once a month said that they had the right to cancel the order, compared to just 33 per cent of those who shopped online a couple of times a year.[176]

[172] OFT (2006a).

[173] The established social grades referred to here are: A (Upper Middle Class, Higher managerial, administrative or professional); B (Middle Class, Intermediate managerial, administrative or professional); C1 (Lower Middle Class Supervisor or clerical and junior managerial, administrative or professional);C2 (Skilled Working Class, Skilled manual workers); D (Working Class, Semi and unskilled manual workers); E (Those at the lowest levels of subsistence, State pensioners, etc, with no other earnings).

[174] Indeed this may overstate levels of awareness because online survey respondents tended to be more likely to have experience of buying online.

[175] OFT (2006b).

[176] Although it is important to note that these were respondents to ePanel, who tended to be more IT literate individuals and on average more likely to have shopped online than respondents to our telephone survey, who were more representative of the general population. These results therefore are likely to overstate awareness compared to the general population.

6.31. However, even the most experienced internet shoppers were still largely unaware of their rights. For instance, 52 per cent of the most regular and largest spenders were unaware of their right to a cancellation period – only four per cent lower than for all internet shoppers (this is not a statistically significant difference). We conclude that reliance on increasing uptake of online shopping is not sufficient to raise consumers' awareness of their rights.

6.32. As we noted in Table 6.1 above, generally, consumers who use their credit card to make purchases of over £100 but less than £30,000 may make a claim under the Consumer Credit Act 1974 ('CCA') against their credit card company for any breach of contract or misrepresentation. See Box 6.3 below.

**Box 6.3: Section 75 Consumer Credit Act 1974**

Section 75 provides shoppers with additional protection if they use a credit card to pay for goods or services between the value of £100 and £30,000. Section 75 provides that if a consumer has a valid claim against a supplier for breach of contract or misrepresentation, they will have a like claim against the card issuer/lender, who is jointly and severally liable with the supplier.

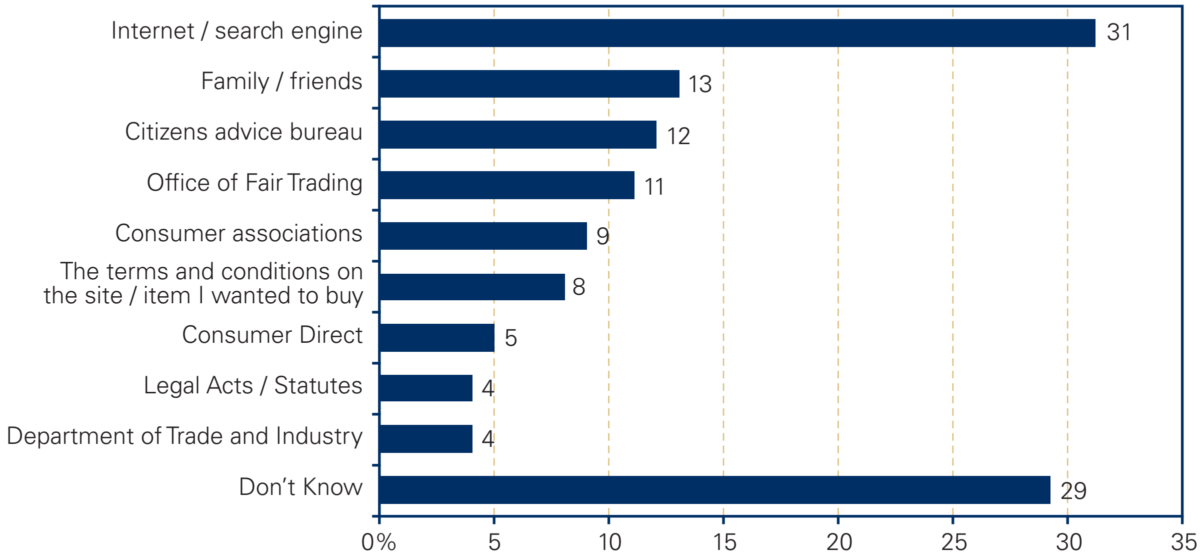
6.33. However, we found that many consumers were also unaware of this protection and some had a (false) belief that they were more protected using a credit card offline than online. Of those who had a credit card, 76 per cent believed they had such protection when shopping offline, but only 65 per cent believed this protection existed online. Furthermore, 27 per cent did not know if they had this protection when shopping online and eight per cent thought they were not protected. There was also confusion over the spend required: only 31 per cent gave the correct answer of £100, with 30 per cent not knowing and one in five (21 per cent) thinking the amount varied.

6.34. It is important that consumers are aware of their rights under the CCA, whether buying online or elsewhere. Our data suggests that people may be less aware of their rights when shopping online, and may be more likely to bear the costs when they have a valid claim for their money back.

### Where do consumers go for advice?

6.35. Our survey showed that internet users were most likely to turn to the internet or search engines if they needed advice about their rights when shopping online, with 31 per cent saying that they would look there. However, a high proportion (29 per cent) did not know who to turn to, suggesting that greater publicity of advisory sources is needed if consumers are to be well informed about their rights.

**Chart 6.2: Where internet users would seek advice on their rights when shopping online**



Source: OFT Consumer telephone survey

Base: All internet shoppers, and non-shoppers who are concerned about security

6.36. Furthermore, 13 per cent said that they would be most likely to ask their family or friends. Survey respondents who indicated that they had more concerns about shopping online were more likely to seek advice from family and friends on what rights they had. This was also borne out in the focus groups, where those who were reluctant to shop online were generally more distrustful of online sources of information and advice. Many felt that internet advice was biased towards getting them to use the internet more frequently, and was not sufficiently independent.

6.37. Services such as Citizens' Advice and Consumer Direct, offer tailored advice on what to do if someone has experienced a consumer related problem, such as when purchasing goods online (see Chapter 8 for more on the role of Consumer Direct). There is also a wide range of potential sources of advice on internet shopping and general surfing. These vary from the formal (informational websites) to the informal (such as blogs), the governmental to the non-governmental. As we identified in Chapter 4, many address issues such as how consumers can protect themselves against security and privacy problems (as well as inappropriate content). Some explain the specific rights consumers have in the online marketplace.

6.38. But although very useful, advisory sources can vary in their scope, purpose and the types of issues they highlight. Furthermore, it seems that many people remain unaware of their rights when shopping online. This suggests that there may be a need for a more tailored and targeted approach, making full use of the internet itself as a tool for dissemination and signposting, as well as working with third parties involved in internet shopping.

6.39. Many people turn to the internet as a search tool for advice. A total of 20 per cent of shoppers with concerns said that they would consult either the OFT, Consumer Direct or DTI for advice on their rights. This suggests that a single source of dedicated, consolidated and impartial advice, or a respected signpost, might be used by many shoppers – particularly if it appeared prominently in internet searches when consumers keyed in typical queries.

## How aware are businesses of consumer rights?

6.40. In our survey, nearly three in ten (28 per cent) of traders currently selling online said that they were not at all aware or only slightly aware of the laws applying to internet shopping. Many of those we spoke to felt that larger businesses were better placed to absorb fully their obligations. To some degree, this was supported by the results of our business survey, which found that 26 per cent of businesses with more than 50 employees considered that their awareness was slight or none, compared with 36 per cent of businesses with fewer than ten employees.[177] It is, however, a concern that so many businesses, whatever their size, said that they had limited or no awareness of their legal obligations to consumers.

### Businesses' awareness of consumer rights

6.41. We focused on the role of the DSRs and the ECRs. Fifty-four per cent of businesses selling online or considering doing so, thought there were specific regulations that covered online shopping. Although not a critical measure of awareness, we found that few of these businesses knew the names of the regulations. Specific regulations of which these businesses were most aware were the DSRs (13 per cent) and the Data Protection Act (9 per cent).

6.42. To test businesses' actual awareness of online shoppers' rights, we asked respondents to our business survey in the electrical and music sectors some questions about hypothetical scenarios involving cancellation (see Table 6.3).

6.43. Electrical items are one of the most popular categories of goods to be sold on the internet. The nature of these goods is such that consumers may want to return them if they discover their purchase is not what they wanted. When we surveyed the awareness of electrical retailers who were selling online about a consumer's right to reject goods that were not faulty, we found that 20 per cent said consumers did not have a right to cancellation, or did not know.

[177] This result is only marginally significant at the 95 per cent level.

Table 6.3: Electrical and musical retailers' awareness of regulations on the return of goods bought online (correct response is in bold type)

| Consumer rights | Electrical retailers selling online (%) | Musical retailers selling online (%) |
|---|---|---|
| Do consumers have a right to cancel… | | |
| **Yes** | **80** | **73** |
| No/Don't know | 20 | 27 |
| Window for cancellation after delivery…[178] | | |
| Up to six days | 1 | 9 |
| **seven days** | **48** | **24** |
| More than seven days | 45 | 47 |
| Don't know | 6 | 22 |
| When must refund be made…? | | |
| **ASAP after cancellation no later than 30 days** | **13** | **8** |
| ASAP after return no later than 30 days | 79 | 86 |
| Don't know | 7 | 5 |
| Can supplier withhold cost of outward delivery… | | |
| Yes | 57 | 51 |
| **No** | **27** | **27** |
| Don't know | 16 | 22 |
| Can supplier withhold restocking/admin fee… | | |
| Yes | 43 | 22 |
| **No** | **45** | **51** |
| Don't know | 12 | 27 |

6.44. Of those electrical retailers who were aware of the cancellation right, only 48 per cent correctly identified seven working days as the correct period. On the other hand, only one per cent thought the period was shorter, meaning that although many businesses were not aware of the correct period, many in fact implied in their responses that their businesses might be giving greater protection than that required in the regulations.

6.45. However, we also found that other aspects of the regulations were not well understood by respondents. For instance:

- when a consumer has properly notified cancellation of an order and requests a refund, the DSRs require it to be processed as soon as possible (and in any case within 30 days): a merchant cannot make people wait until they have received the goods back. However, only 13 per cent of online electrical retailers were aware of this requirement
- most (57 per cent of electrical retailers and 51 per cent of music retailers) wrongly thought they could withhold the cost of outward delivery
- forty three per cent of those electrical retailers who were aware of the right to return wrongly thought they could withhold a restocking or administration fee.

[178] The correct answer is seven working days, but for simplicity the questionnaire stated seven days.

6.46. The DSRs require the name and address of the business (if payment is required in advance) to be provided in a clear and comprehensible manner in good time before a consumer contracts with the business.[179] The ECRs also require that businesses give a name and geographical address as well as an email address to enable direct and rapid communication.[180] However, our survey of businesses also revealed gaps in knowledge of these legal requirements: a fifth (21 per cent) did not think they had to provide their email address, and a quarter (24 per cent) did not think they had to provide their geographical address.

## Businesses' compliance with the regulations

6.47. The survey findings suggested the possibility that many retailers, through poor awareness, might not be complying with consumers' rights. However, to assess whether businesses actually complied with the regulations, we also commissioned a survey of UK sites selling to UK consumers. The review looked at 250 websites in total from across the electrical, travel and music sectors. The reviewers often had difficulty locating the information required by the regulations. Because sites were set up in a number of different ways, investigators had to search many different pages to find the information they were looking for, in the same way that a consumer would have to.

6.48. Similar surveys such as that conducted by Norfolk Trading Standards in 2005 found the number of fully compliant websites to be low – echoing an earlier exercise conducted by the OFT in 2001, which looked at 637 sites and found 52 per cent were non-compliant.

### Provision of contact details

6.49. Our review found some variation between the methods employed to enable consumers to communicate with the retailer. Table 6.4 shows that electrical goods manufacturers more often supplied an email address whereas music retailers were more likely to have a web form than an email address.[181] Sixty one per cent of flight vendors provided an email address and 31 per cent had a web form, suggesting that they may rely more on telephone contact (provided by 91 per cent).

6.50. These results suggest that, of the sites examined in our review, 20 per cent of electrical retailers' sites, 39 per cent of sites selling flights and 46 per cent of music retail sites may be breaching the regulations by apparently not providing an email address. Weak awareness and lack of compliance in providing contact details is a concern, given that problems contacting or communicating with traders was the second most cited difficulty for consumers who had experienced a problem buying online in the 12 months to November 2006 (14 per cent).

[179] Regulation 7(1)

[180] In addition, The Companies (Registrar, Languages and Trading Disclosures) Regulations 2006 which came into force earlier this year require a company to provide details on all its websites of its place of registration and number, the address of its registered office, and to indicate whether it is a limited company or an investment company.

[181] Whilst a web form may be a convenient means of communication in some situations, the ECRs require the service provider to make available to the recipient of the service, in a form and manner which is easily, directly and permanently accessible, his name, geographic address and his details, including his electronic mail address, which make it possible to contact him rapidly and communicate with him in a direct and effective manner. In our view, a web form without an electronic mail address will not satisfy this requirement.

### Table 6.4: Business contact details provided

| Business contact details provided | Electrical (100) % | Music (50) % | Flight (100) % |
|---|---|---|---|
| Full geographical main business address | 93 | 80 | 73 |
| Contact telephone number in event of a problem | 90 | 58 | 91 |
| Email address for consumer services | 80 | 54 | 61 |
| Web form can be submitted by consumer | 63 | 66 | 31 |
| Fax number | 54 | 40 | 32 |
| PO Box number | 9 | 12 | 7 |
| Proportions giving EACH of the first five contact details | 23 | 6 | - |
| Proportions giving main business address AND email address or web form | 91 | 70 | 54 |

### Availability and retention of terms and conditions

6.51. The ECRs require that where retailers provide terms and conditions to consumers, they do so in a way that allows them to store and reproduce them. We did not undertake test purchases and therefore did not test whether or not retailers satisfied this requirement by, for example, providing a printed receipt containing the terms and conditions at the same time as the delivered product (in the case of deliveries). However, our review did find that terms and conditions were relatively easy to find and to read.

### Table 6.5: Terms and conditions

| Sector | Terms and conditions found % | Easy to find % | Easy to read % |
|---|---|---|---|
| Flights (100 sites) | 98 | 89 | 97 |
| Music (50) | 94 | 88 | 90 |
| Electrical (100) | 92 | 84 | 90 |

### Cancellation period

6.52. For our case study sectors, the cancellation period contained in the DSRs applies to the electrical goods and music vendors, but not to flights. We found that of the three sectors, electrical goods retailers gave the fullest information on cancellation in an easy to find form, but nearly a quarter of music retailers' sites (24 per cent) appeared to make no mention of a right to cancel hardcopy purchases.[182] Our review also found that information on cancellation was easier to find on the electrical retailers' sites than on the music retailers' sites.

6.53. Where electrical retailers' sites mentioned a cancellation period, most (84 per cent) appeared to give shoppers seven working days or more – apparently meeting or exceeding the requirements of the regulations. However, the reviewers also found that 12 per cent of electrical sites appeared not to mention any cancellation period and four per cent seemed to say it was less than seven days. Also 39 per cent of music retail sites appeared not to mention a period or said there was no right to cancel.

[182] Unless traders agree otherwise, consumers cannot cancel if the order is for audio or video recordings or computer software that the consumer has unsealed (DSRs, Regulation 1391)(d)).

Table 6.6: Cancellation information

| Cancellation information | Electrical<br>(100 sites)<br>% | Hard copy music<br>(46 sites)<br>% | Flight<br>(100 sites)<br>% |
|---|---|---|---|
| Mention of cancellation period | 88 | 61 | 25[183] |
| Explanations of how to cancel order | 94 | 76 | 63 |
| Information easy to find and understand | 84 | 68 | 62 |

6.54. We also found that many sites may have given consumers the impression that their rights were limited (in fact, consumers can only be required to take 'reasonable care' of the goods throughout the cancellation period). All but six per cent of the electrical sites examined appeared to attach conditions to returns. Some typical conditions which may have led to a breach included:

- goods to be returned/collected unused (on 33 per cent of sites)
- goods to be returned/collected 'as new' (on 17 per cent)
- goods to be returned/collected unopened (on 10 per cent)

6.55. Indeed, of the 100 electrical websites reviewed, 59 per cent stated at least one condition on consumers' rights to cancel and receive a refund which, depending on the circumstances, may have meant a breach of the regulations.

### Complaints handling

6.56. Overall the number of websites describing a complaints handling process was low. Fewer than half of electrical retailers (44 per cent) and flight vendors (43 per cent) described a complaints process on their websites and only 10 per cent of music retailers did so. Pure internet retailers of electrical goods did slightly better, with 50 per cent describing a complaints process. It is, however, possible that retailers may have provided this information at a later stage, for example with the invoice.[184]

### Guidance for businesses on consumer rights

6.57. Overall, businesses' levels of awareness of, and compliance with, their consumer protection obligations for online trading could clearly be better and the provision of clear guidance is, of course, an important factor. Although the majority (77 per cent) of online traders we surveyed said that there were no areas on which they needed more guidance on the law, of the 19 per cent who did say they required more guidance:

- 21 per cent said they wanted more information on consumer rights
- 20 per cent wanted guidance on the law surrounding returns
- 12 per cent wanted advice on data protection issues.

[183] Note that the cancellation period in the DSRs does not extend to travel services.

[184] For practical purposes, our websites review did not include test purchases: it did not go beyond testing the contents of websites up to point of payment. The issue of test purchases is discussed in Chapter 8 on enforcement.

6.58. We found that of the online traders that had sought advice, the largest number (28 per cent) had turned to a lawyer, followed by 16 per cent who relied on their trade association and an equal proportion used the internet itself. For those who had not sought any advice the largest proportion, one in four (25 per cent), said that they would turn to the internet in the first instance.

6.59. When we surveyed businesses with websites to see if they used content from other sites to set up their own, 32 per cent said they did. Stakeholders also confirmed that some businesses copied terms and conditions from established retailers to save on costs. This raises the prospect of non-compliance spreading from site to site.

6.60. In our business survey, 31 per cent (the highest proportion) said that a single source of guidance on online shopping would most improve awareness, and 21 per cent said more concise guidance would help. Those businesses we met confirmed that a proliferation of advisory sources on the internet could be counterproductive.

6.61. There are, indeed, many sources of advice available to online businesses, covering issues from security through to consumer protection, accessibility and tax advice. We listed examples of those relating to security in Chapter 4 and some of these provide other information, including on consumer rights. Examples of public sites include (there are also many private sites):

- **Business Link** – www.businesslink.gov.uk/bdotg/action/detail?type=RESOURCES&itemId=1075742593
- **OFT** – www.oft.gov.uk
- **DTI** – www.dti.gov.uk/consumers/fact-sheets/page38102.html
- **ICO** – www.ico.gov.uk/upload/documents/library/data_protection/practical_application/getting_it_right_a_brief_guide_to_data_protection_for_smes.pdf
- **HMRC** – www.hmrc.gov.uk/guidance/selling/index.htm

6.62. One business interviewee commented:

*'I think that would be fantastic because there are a number of places where you can get information about the internet but it does tend to be quite disparate. It's not all contained in one place and it's kind of split between industry bodies and consultancy firms. So I think it would be good to have it all contained in one place.'* (National Music Retailer)

6.63. However, and of more concern, 66 per cent of businesses currently selling online told us that they had never even sought advice on their obligations to consumers when selling online (a figure which increased to 75 per cent for businesses with fewer than 10 employees). Approaches that rely on users wanting to find and use websites cannot alone address poor awareness in these circumstances. This seems particularly the case given the poor awareness and examples of non-compliance we identified, despite three-quarters of online traders (77 per cent) saying that they did not need more guidance.

6.64. We cannot be certain that weak awareness and compliance lies behind many of the problems consumers have experienced, described in Chapter 5. However, it is likely to be an important factor in many cases where, for instance, consumers have had difficulty communicating with a trader or in returning goods.

6.65. More needs to be done in an active way to help businesses to know and understand consumer rights. One way to direct advice to businesses would be via the third parties that they have most contact with when establishing an online presence – legal advisors, ISPs, trade associations and web developers. For instance, we found that 16 per cent had sought advice from their Trade Association and 11 per cent from their web designer: more than had contacted Trading Standards Services (nine per cent) or the OFT (six per cent).

## Conclusions

6.66. Although the key regulations appear broadly fit for purpose at present, we identified a number of areas where they could need updating, which we have brought to the attention of the European Commission.

6.67. We found that most people (56 per cent) did not know about their right to cancel, and many (29 per cent) also did not know where to turn to get advice on their rights. More worryingly, we found that a lot of traders had a weak awareness of the law themselves, and that some websites may have been breaching them.

6.68. Businesses told us that guidance on the key legal requirements should be clearer and have a higher profile – preferably with a single clear, dedicated source or signpost.

### Next steps

6.69. We will develop and implement a strategy employing the most effective and innovative ways actively to raise business and consumer awareness of online shoppers' rights – both directly and by working with third parties. We will also look into whether and how the wider range of relevant advice to internet traders and buyers could be more co-ordinated. We will encourage industry to self-assess, to make sure it is complying with the relevant legislation. Enforcement may ultimately be considered, to target outstanding breaches that create clear detriment.

# 7 CODES OF PRACTICE

## Summary

One factor that shoppers might sometimes consider is whether a business is signed up to a code of practice and whether, should something go wrong, they can approach the relevant body for redress. The concerns some consumers have about online shopping would seem to make membership of consumer codes of practice a potential way for traders to overcome consumer fears about their reliability. However, there has been only slow and limited take up to date of online codes of practice.

There are clearly potential barriers to the establishment and growth of such codes, such as logo protection and code enforcement. However, while some stakeholders expressed scepticism about them, others felt they were the best way to regulate the internet and raise confidence. Most who commented wanted the industry to regulate itself rather than be subject to significant external regulation – many felt this was key for such a relatively new and dynamic market.

There does appear to be some scope for a greater role for codes of practice, in the form of both dedicated online codes (or 'trustmark schemes') and those sectoral codes that also cover online sales. Many businesses that signed up to a code see benefits and, where consumers recognise a code, they associate it with more security suggesting that they may help businesses to sell. Lack of awareness rather than scepticism seems to be the main barrier to their development. There may also be scope for some sectoral codes largely addressing offline sales to cover online sales too. This could help to raise consumer and business awareness of the regulations governing internet shopping; helping to share the enforcement role with industry more effectively.

## Next steps

We want to continue to encourage sponsors of dedicated online codes of practice to consider applying under the OFT's Consumer Codes Approval Scheme (CCAS), and to find ways to raise the profile of such codes for consumers and businesses. We also want to discuss further with code owners for offline traders the potential for enhancing how they cover the online activities of those members who also trade online.

## Introduction

7.1. Elsewhere in our study, we note examples of specific self-regulatory practices with potential value to internet shopping. For instance, in Chapter 4, we discuss the role of the Banking Code, while in Chapter 9 we address the British Code of Advertising, Sales Promotion and Direct Marketing (the 'CAP Code').

7.2. Codes of practice are another form of industry self-regulation which can help raise consumer confidence in dealing with their member traders, as well as providing redress mechanisms when something goes wrong. We consider in this Chapter their potential role, given the confidence and redress issues we have identified in the study.

## Codes of practice and internet shopping

### The role of consumer codes of practice

7.3. The OFT has adopted a clear position on consumer codes of practice, through its Consumer Codes Approval Scheme (CCAS). Our view is that effective codes should set clear standards of business practice, and be effectively monitored by their owners for the mutual benefit of consumers and those businesses that sign up to them.

7.4. We believe that effective codes, such as those approved under the CCAS, can help to address sector or channel-specific problems and can lead to increased standards of customer service across industry sectors, as these voluntary standards are increasingly adopted and exceeded in order to attract and retain customers. While codes do not directly address the problem of rogue traders (discussed in Chapter 8), they may help to marginalise them, allowing those involved with enforcement to target their resources more effectively.

7.5. Industry codes typically apply to particular sectors of industry – for example, the motor trade or estate agencies. Although the internet is a sales channel rather than a market sector, there are also codes which relate specifically to the sales channel in which businesses operate. For example, the Direct Selling Association (DSA) operates a code of practice for retailers selling goods directly to consumers (see Box 7.1). And, there are several dedicated 'online codes' in existence, including that administered under the SafeBuy Assurance Scheme for Web-based Traders[185] which has completed Stage One of the two-stage process under our Consumer Codes Approval Scheme (CCAS).[186]

### Box 7.1: The DSA code of practice

An example of a code that operates in a sales channel is that of the Direct Selling Association. The DSA's members supply a wide range of goods and services but share the common sales channel of direct selling (most commonly by taking face-to-face orders following the delivery of a catalogue).

The DSA code, which is approved by the OFT under the CCAS, is administered by an independent code administrator and provides customers with benefits that go above and beyond legal requirements when shopping at home. These include superior cancellation rights to those available at law and access to an independent redress mechanism should something go wrong.

[185] The SafeBuy Assurance Scheme for web-based retailers is operated by Software Research Ltd. The SafeBuy code of practice completed Stage One of the CCAS in February 2006.

[186] The CCAS consists of two stages. During Stage One the code must meet the OFT's published core criteria, which contain measures designed to remove or ease consumer concerns about undesirable trading practices. In Stage Two the code sponsor must prove that its code lives up to the promises made in Stage One by demonstrating that the code is being effectively implemented by its members and that consumer disputes are properly resolved. Once the two stage process is complete businesses can display the OFT Approved code logo together with the code sponsor's logo.

## The Consumer Codes Approval Scheme (CCAS)

7.6. The aim of the Consumer Codes Approval Scheme (CCAS) is to promote and safeguard consumers' interests by helping consumers identify better businesses and to encourage businesses to raise their standards of customer service. The OFT endorses and promotes those codes that can demonstrate they are providing real benefits, above and beyond legal requirements, to consumers. There are currently five OFT approved codes, and several others part way through the approval process.[187]

## Domestic self-regulation and internet shopping

### History of online codes

7.7. Codes have had a relatively low impact on internet shopping to date, both in terms of business take-up and consumer awareness. This is despite several attempts since the late 1990s to establish them through trustmark schemes, with the aim of increasing consumer confidence in online shopping.

7.8. These schemes typically lay down a set of conditions, usually in the form of a code, for online trading – including pre-contractual information security, advertising, cancellation rights and complaints handling. In return members are entitled to display the logo associated with the trustmark scheme.

7.9. Although most of these schemes have met with only limited success, the Which? Web Trader scheme, operated by Consumers Association[188] and free for businesses to join, attracted more than 2,700 members and resolved around 2,000 disputes in less than four years of operation. However, it folded in 2003 on the grounds of being too costly to run. Furthermore, the industry-led Trust UK[189] scheme was closed this year by the Direct Marketing Authority (DMA), which oversaw its operation.

7.10. Experiences of self regulation in other countries seem similar. Trustmarks are a feature of online trade in two thirds of EU countries. Examples include L@belsite (France) and Trusted Shops (Germany). Outside the EU, examples include the DMA (Japan); and the Better Business Bureau (BBB) in US which runs a scheme whereby online businesses that conform to certain criteria may place a 'Reliability Seal' on their websites.[190]

7.11. Furthermore, 'Consumer Reports WebWatch' is a project of Consumers Union which seeks to raise the credibility of content on the Web, by conducting research and producing guidelines for best practice, which it encourages industry to sign up to. It also runs an 'e-Ratings' scheme, rating websites on categories such as disclosure of transaction fees, clarity of privacy policies, how clearly advertising is labelled etc.

[187] The codes of the following bodies are OFT approved: The Society for Motor Manufacturers and Traders (New car warranties code), the Vehicle Builders and Repairers Association Ltd, the Direct Selling Association, the Ombudsman for Estate Agents Company Ltd and the Carpet Foundation.

[188] Now known as 'Which?'

[189] Trust UK was set up by industry in 1999 in an attempt to bring together the wide range of schemes and hallmarks that were being developed at that time.

[190] Currently, over 34,000 websites qualify to display the Reliability seal. For more information, see www.bbbonline.org/reliability/Rel_EN.asp

7.12. While some of these schemes are large, many have a relatively small penetration in terms of membership.[191] In our consultation of ICPEN members, the Danish Consumer Ombudsman told us that a web sweep of the 354 sites signed up to their 'e-mark' showed that members were more compliant with regulations than non-members. Otherwise, however, evidence of the effectiveness of such schemes is lacking. Australia had assessed internet shopping trustmarks in 2005 and reported low awareness and little effectiveness.[192]

### Current dedicated online schemes

7.13. Our consideration of current domestic schemes was restricted to those that appeared to operate a reasonably robust business to consumer code (although it should be noted that the OFT is yet to approve a dedicated online code under the CCAS). There are currently two schemes that have achieved more than 1,000 subscribers and one smaller scheme:

- the Internet Shopping Is Safe (ISIS) scheme, operated by the Interactive Media in Retail Group (IMRG), which has around 1,200 accredited retailers;
- the SafeBuy Assurance Scheme[193], which has around 1,200 subscribers and 1,500 accredited websites; and
- the DMA-operated WebTraderUK Scheme, which has about 200 members.

7.14. There is some evidence to suggest that the nature of different product sectors may play a part in the take up of these schemes. For instance, our websites review revealed that electrical retailers appeared to buck the general trend, with 43 per cent members of one of the main schemes.

7.15. However, penetration overall seems modest. We found membership of such schemes is limited to less than 10 per cent of online traders, and is slow growing. One scheme owner, for instance, told us that it had an estimated 2 to 2.5 per cent of the market.

## Potential barriers to the take-up on online codes

7.16. To understand the low take-up to date, we considered some of the potential barriers to the growth of schemes cited by stakeholders and commentators – some of which seem more significant than others:

- Lack of awareness
- Lack of incentive for big businesses to support codes
- Costs
- Logo proliferation and protection
- Difficulties in enforcing codes
- Perceptions of weak regulatory enforcement
- Alternative information sources unique to the internet

[191] Trzaskowski (2006) reported that the largest of the European trustmarks surveyed, the German Trusted Shops, had approved 'more than 1500 shops', but most had fewer than 100 members.

[192] Consumer Affairs Victoria (2005).

[193] SafeBuy's code of practice has completed Stage One of the OFT's Consumer Codes Approval Scheme.

### Lack of awareness

7.17. There is low awareness amongst both businesses and consumers alike of online codes of practice. For consumers, only 24 per cent of respondents to our online survey looked for membership of any code when shopping online.[194] And of the 76 per cent of consumers who did not look for a code, the main reason was they were unaware of them or their role (75 per cent).

7.18. There was also generally low awareness of particular schemes. When presented with a list of logos representing various types of schemes intended to raise consumer confidence, 21 per cent of consumers recognised ISIS; nine per cent SafeBuy; and eight per cent recognised TrustUK or WebTraderUK. In contrast, logos relating to travel and financial protection tended to have higher rates: 69 per cent for ABTA, 61 per cent for Verisign, and 43 per cent for Verified by Visa.

7.19. In general businesses had higher levels of recognition: 30 per cent recognised TrustUK; 27 per cent WebTraderUK[195] and 21 per cent SafeBuy. But again recognition of scheme logos was well behind other long-established logos such as ABTA (76 per cent); ATOL (65 per cent); and Verisign (48 per cent). Business awareness of one particular scheme; ISIS (25 per cent), was similar to the proportion of consumers who recognised it (21 per cent). Businesses most commonly cited a lack of awareness of trustmark schemes as their reason for not signing up to codes (21 per cent), although 32 per cent did not have a reason.

7.20. The difference in levels of recognition is perhaps not surprising when comparing trustmark scheme logos to brand names, some of which have been well known for years online and offline. However, it is clear that there is some way to go for these schemes to achieve significant levels of recognition – although it is encouraging that the ISIS brand was nearly as well recognised by consumers as that of MasterCard SecureCode. This suggests that it is feasible to build up rates of recognition.

### Lack of incentive for big businesses to support codes

7.21. The view that membership of a trustmark scheme would be more likely to benefit SMEs than branded retailers was common amongst stakeholders. It was felt that in order for a self-regulatory scheme to be effective it has to be seen as a brand in itself, which smaller traders can benefit from and use to compete with larger businesses. To date, no trustmark scheme appears to have established a high enough profile to compete in this manner. Promotion, therefore, appears to be integral. If consumers are not aware of the benefits of trustmarks they are more likely to rely on branded retailers.

7.22. It follows that larger players may potentially gain from the absence of a well known alternative 'brand' and thus have less incentive to join and back a trustmark scheme. Some stakeholders suggested that big brand names were not interested in codes because they have invested in their brand names already and already enjoyed the level of trust that a code would bring.

7.23. This can be viewed as a market based response to consumer concerns about shopping online – high street retailers have extended their sales online and this has encouraged nervous shoppers – but that does not help small firms who struggle to earn the trust of consumers. Where consumers have disproportionate fears about shopping online and do not shop with new and small firms they could be missing out on a wider choice and potentially lower prices (see Chapter 9).

[194] This may also overstate the picture for all consumers since online survey respondents are more experienced internet users.

[195] Note however, that there may have been potential for confusion between the similar-sounding 'WebTraderUK' scheme, and the redundant 'Which? WebTrader' scheme.

## Costs

7.24. Some organisations suggested that effective trustmark schemes are costly to run and that, inevitably, this cost is passed on to member businesses. Furthermore, this is a particular issue for online shopping because SMEs may be potentially more able to bear the costs of setting up online than offline, but have tighter budgets. Code owners told us that compliance monitoring, particularly with regard to the checking of IT equipment, and the provision of a complaint handling service can be the costliest aspects of operating these schemes.

7.25. However, although there may be cost issues for scheme operators, the cost of joining seems to be less of an issue for potential business members. Membership costs are relatively low: annual subscription fees for the major trustmark schemes range from £95 to £350 (plus VAT). Only four per cent of businesses surveyed cited expense as a reason for not signing up to a code scheme; with only six per cent saying they would join if schemes were cheaper.

## Logo proliferation and protection

7.26. Websites often have many labels and symbols relating to a range of issues, for example, security and membership of various bodies. Given this, some stakeholders have suggested that trustmark schemes reliant on logo-recognition find it difficult to establish themselves. However, this seemed to be less of a concern for businesses: only two per cent cited too many schemes as the reason for not signing up. Also, the 21 per cent recognition rate among respondents to our online consumer survey of the ISIS logo, which started in July 2001, suggests that it is possible to build awareness.

7.27. However, some businesses felt that logos were too easy to 'lift' on the internet. Logos are easy to copy, although internet verification schemes have worked for some years (such as Verisign and certificates), suggesting that logo copying may not be an insurmountable barrier, although clearly it would require effective policing. If trustmark schemes gained momentum, however, their respective memberships could become increasingly motivated to help police misuse.

## Difficulties in enforcing codes

7.28. Code owners (and consumer bodies) said that trustmark schemes faced the same problems as formal regulators (discussed in Chapter 8) – that websites can set up and close down quickly; falsely claim membership; and owners can be hard to track down.

7.29. These factors do appear to be valid concerns about the potential for such schemes. They suggest that consumers would need to be made aware of the benefits to check for when considering the value of a trustmark, as well as a role for enforcers to make clear which schemes meet minimum standards. They also underline the potential value of schemes like the CCAS which set clear standards that codes are required to meet in order to be approved.

## Perceptions of weak regulatory enforcement

7.30. Many stakeholders thought enforcement for online shopping to be too weak or low profile (enforcement is addressed in the next Chapter). Some argued that until enforcement was seen to be effective, businesses would not take regulations seriously and would be unwilling to pay for the 'insurance' offered by codes. In contrast, however, many also argued that codes were more flexible and better suited to dealing with the dynamic online shopping market than 'heavy-handed' regulation and enforcement.

### Alternative information sources unique to the internet

7.31. Some businesses argued that there was less potential or need for codes given the development of alternative information sources unique to the internet, such as user reviews and customer ratings facilities. Such facilities have become a popular tool for internet traders and are a feature of many established internet brands. Feedback systems are a particular feature of online auctions (see chapter 10) in the form of reputation systems. They also feature heavily on price comparison sites in the form of consumer rankings of retailers and products and, to a lesser extent, on individual traders' websites.

7.32. Most stakeholders see value in feedback systems and view them as an effective way to drive good behaviour by business and empower consumers, and a number said that consumers place a certain degree of trust in them. They often provide a simple and speedy way for consumers to judge traders. However, several stakeholders also voiced their concerns about the potential for manipulation of feedback, either through beneficial self-rating by businesses, or by 'guerrilla marketing' tactics by competitors who leave fictitious, adverse comments on sites.

7.33. One stakeholder suggested that smaller companies may be better able to manipulate reviews due to the small number they receive. Some stakeholders informed us that they actively police their sites for evidence of manipulation and that this can lead to expulsion, but others were less clear how to effectively go about this. Another common view amongst stakeholders was that reviews have the tendency to be polarised between either very good or very bad. This is perhaps indicative of the fact that consumers are more likely to report either very positive or very negative experiences than they are to report an average one.

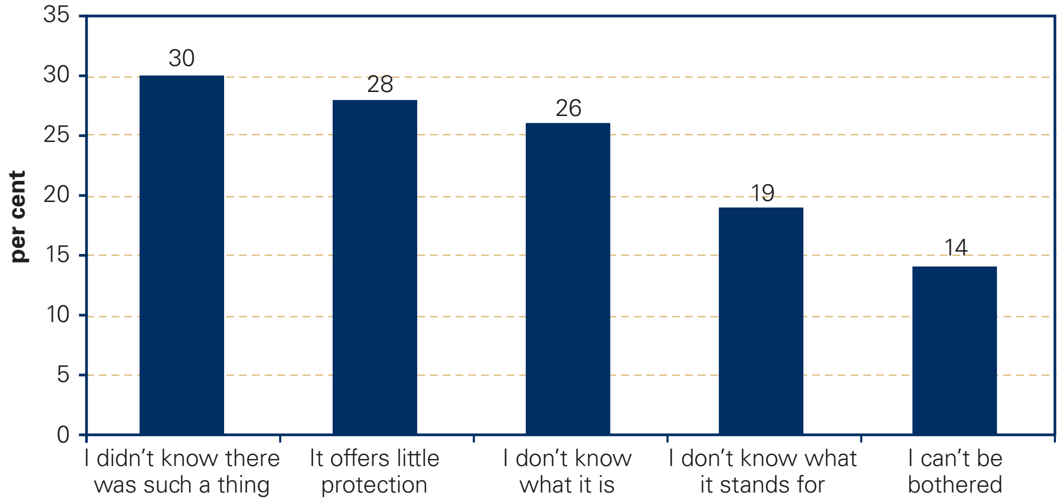
7.34. While feedback systems have a valuable role to play in raising consumer confidence in online shopping, they do not necessarily replace the value of effective codes. Not all online consumers use price comparison websites (27 per cent had not used one in the 12 months prior to our survey) and it is unclear what proportion of users actually rely on the reviews. Unlike an effective code, feedback systems alone do not provide a safety net for consumers that encounter problems in the form of a dispute resolution service; nor do they provide a mechanism for monitoring or enforcing compliance with a set of standards or regulatory obligations or provide a clear signpost of the standards that a trader has promised to adhere to.

## The potential value of self regulation

7.35. There are clearly potential barriers to the establishment and growth of online codes of practice. However, while some stakeholders expressed scepticism about them, others felt they were the best way to regulate the internet and raise confidence. Most who commented wanted the industry to regulate itself rather than be subject to significant external regulation – many felt this was key for such a relatively new and dynamic market.

7.36. Of the businesses we surveyed the most cited reason for not having joined a scheme was lack of awareness (see paragraph 7.17), rather than costs (see paragraph 7.25) or scepticism (only 14 per cent said it would not improve their business). Likewise, most consumers were unaware of codes (75 per cent did not know about them, did not know what they were, or what they stood for), rather than sceptical (only 28 per cent believed they offered little protection).

**Chart 7.1: Why shoppers in our online survey did not look for a code of practice**



Source: OFT Consumer online survey

Base: All respondents who do not look for a code of practice

7.37. There was also recognition of the potential value of codes: businesses surveyed who were already members of a code listed the main benefits as: raises consumer confidence (47 per cent); improves credibility (20 per cent); helps them address problems (13 per cent) and also aids their understanding of regulations (12 per cent).

7.38. Furthermore, there is evidence that consumers notice online logos – for example, 70 per cent of online survey respondents indicated that they looked for the security padlock symbol when buying online. However, when questioned further, very few people actually understood what the symbol meant and what the implications for the transaction really were. This demonstrates both the potential value online codes with easily identifiable logos could have and their limitations if they are not adequately promoted.

7.39. Consumers who recognised specific codes related them to security, reassurance and protection. In its 2005 report on internet shopping,[196] the Welsh Consumer Council (WCC) concluded that trustmarks can reassure consumers that the website they are using meets a benchmark for consumer advice. They stated that IMRG's ISIS scheme had been successful in the UK in promoting a greater sense of online security and trust among consumers. One major trustmark operator also told us that code members reported a greater ratio of sales to hits on joining the scheme.

7.40. IMRG found that many consumers fell out of an online transaction at the final step of inputting their payment details. While this could be due to consumer scepticism that an accurate overall price would be presented prior to this stage (for instance due either to poor website design or a perceived lack of transparency of additional charges), they also believed that having a logo on the transaction page could give consumers the necessary confidence to go through with a purchase.

[196] Richards (2005).

7.41. There was also evidence of potential interest in codes. Businesses surveyed said that they would be more likely to sign up to one if there was evidence it would boost sales (19 per cent); it was a well-known brand (13 per cent) or government endorsed (11 per cent). Consumers would be more likely to look for codes in the future if they knew more about what the code meant (61 per cent) and if the code guaranteed protection (59 per cent).

7.42. Furthermore, many non-internet codes operate in sectors with heavy and increasing internet sales including travel, vehicle hire and ticket agency sales. In our survey, 27 per cent of businesses selling online said that they were members of other trade associations that had their own code of practice for online selling. It was not clear, however, whether these were dedicated online codes or whether part of a wider scheme, covering offline and online.

7.43. Most sector-based code owners we spoke to felt that their codes either currently provided or had the potential to provide adequate protection for consumers transacting online with their members. However, while some such codes currently contain provisions relating specifically to members' online activities, often in the form of a restating of legal requirements, others remain silent on these matters. There could therefore be potential for code sponsors to raise standards by addressing online sales more explicitly in their codes of practice.

## Conclusion

7.44. We have identified that lack of trust is the biggest issue for consumers when shopping online. A significant proportion of businesses that do sign up to a code believe that membership raises confidence; and our consumer surveys indicate that where consumers recognise a code they associate it with more security. As discussed in Chapter 3, more confident consumers are more likely to transact online. While there is currently a lack of awareness, consumers have indicated that they would look for codes if they understood them better and they offered clear protection.

7.45. There are clearly potential barriers to the establishment and growth of codes of practice, such as logo protection online and their enforcement. However, while some of those we spoke to expressed scepticism about them, others felt they were the best way to regulate the internet and raise confidence. Most who commented wanted the industry to regulate itself rather than be subject to significant external regulation – many felt this was key for such a relatively new and dynamic market.

7.46. There does appear to be some scope for a greater role for codes of practice, in the form of both dedicated online codes and those sectoral codes that also cover online sales. Many businesses that signed up to a code see benefits and where consumers recognise a code they associate it with more security, suggesting that they may help businesses to sell. Lack of awareness rather than scepticism seems to be the problem. There may also be scope for some sectoral codes largely addressing offline sales to cover online sales too. This could help to raise consumer and business awareness of the regulations governing internet shopping; helping to share the enforcement role with industry more effectively.

## Next steps

7.47. We want to continue to encourage sponsors of dedicated online codes of practice to consider applying under the OFT's Consumer Codes Approval Scheme (CCAS), and to find ways to raise the profile of such codes for consumers and businesses. We also want to discuss further with code owners for offline traders the potential for enhancing how they cover the online activities of those members who also trade online.

# 8 ENFORCEMENT AND INTERNET SHOPPING

## Summary

The internet offers an evolving market place with many interested parties, resulting in a complex environment in which to conduct investigations. As internet shopping expands, it is likely to be a growing issue for enforcement.

There are already good examples of enforcement agencies and advisory bodies providing advice to businesses and consumers about online shoppers' rights. We also found some promising examples of proactive work, for instance to assess compliance; to liaise with the internet industry to obtain information on traders; and to co-ordinate activities with other enforcers to achieve successful outcomes.

However, despite these efforts, awareness of and compliance with consumer protection laws specific to distance selling could be better. We see potential for greater co-operation between enforcers so as to ensure greater consistency in how enforcers assess and deal with problems related to internet traders. Good practice should be spread across the whole country.

There is currently no national risk-based approach to identifying problems and aligning the most appropriate response. This needs to be considered within the broader context of other current initiatives which form part of the government's better regulation agenda that will have an impact on local enforcement in general. This includes the establishment of the Local Better Regulation Office (LBRO) with its aim to improve the effectiveness and consistency of local authority regulatory services.

Our research also suggested that enforcement officers face particular challenges in addressing problems related to online shopping – especially in tracing rogue traders. Traders can sell from any location in the UK or abroad and quickly set up or shut down operations. The rapid pace of technological change, coupled with the range of parties that may have an involvement in a transaction also make it a complex environment in which to conduct investigations. Closer working with internet 'gatekeepers', access to pooled skills and more foresight work (to consider future developments) may be some of the ways to help enforcers handle these challenges.

## Next steps

We invite the views of enforcement partners and will explore with them how to enhance enforcement for online shopping in the future. In line with the principles of a targeted, risk-based approach, currently being established for enforcers, an issue for further consideration could be how best enforcers can target their activity according to the greatest risks and potential detriment for online consumers. Other solutions to consider could include:

- working with industry players who may be able to help with tracing website owners
- investigating possible new tools and techniques, and pooling skills and knowledge in centres of expertise for enforcement staff to call upon
- greater central support in identifying national patterns in complaints
- better active monitoring and surveillance approaches, such as those adopted in some other countries
- greater communication and co-ordination between the key agencies

## Introduction

8.1. The internet offers an evolving market place with many interested parties, resulting in a complex environment in which to conduct investigations. This chapter considers whether enforcers have sufficient skills, resources and powers as well as co-operative arrangements in place to regulate the online environment in the most efficient way to the benefit of consumers and honest businesses. Our study covered many issues, so this is inevitably an overview of the enforcement issues, providing a foundation for future work in this area.

8.2. We conducted interviews with case officers in the OFT and Local Authority Trading Standards Services (TSS), and followed these with a survey of TSS. We then held a workshop with TSS and representatives from across the UK and from other agencies with an enforcement interest. We also sought wider stakeholder views on enforcement.

8.3. Our primary focus in this study was on the distance selling nature of the internet and the additional rights online shoppers have. Our survey of TSS, however, provided a picture of the breadth of the challenges faced by TSS in dealing with the internet that span both criminal and civil legislation, which we also reflect in this chapter.

8.4. Finally, we touch upon some key initiatives that are currently impacting on enforcement generally, including the introduction of the DTI-funded Regional Intelligence Network and the establishment of the Local Better Regulation Office (LBRO).

## The enforcement landscape

### The OFT

8.5. The OFT is a non-ministerial government department. Its mission is to make markets work well for consumers. Since April 2006, the OFT has also managed Consumer Direct, the national telephone and online consumer advice service (see Box 8.1).

**Box 8.1: Consumer Direct**

Consumer Direct aims to give consumers clear, practical and impartial advice to help them resolve problems or disagreements with suppliers. The service is delivered by more than 300 staff in 11 contact centres in England, Scotland and Wales (consumers in Northern Ireland are served by the separate but similar ConsumerLine service).

Consumer Direct does not intervene in disputes and nor does it recommend particular suppliers or products. When callers need further help, including face-to-face advice, Consumer Direct refers them to specialist agencies such as their Local Authority TSS or Citizens Advice Bureaux (CAB).

Consumer Direct recently took its three millionth call since the service launched in 2004.

8.6. The OFT has general and specific functions and powers under the Enterprise Act 2002 ('EA2002'), which grants civil powers to general and designated enforcers to seek undertakings and court orders to deal with infringements of certain consumer protection laws (including the DSRs and ECRs) – but only where the infringement harms the collective interests of consumers. The EA2002 also facilitates enforcers taking cross border action in some situations. The OFT's role is to take action on behalf of consumers as a whole and not to seek redress on behalf of individual consumers.

## Local Authority Trading Standards Services (TSS)

8.7. Most enforcement of consumer protection legislation in the UK is performed by TSS in local authorities. TSS investigate a broader range of issues regarding traders than does the OFT. This reflects the broader remit and powers, including criminal powers that TSS can use to protect the interests of consumers.

8.8. As well as DSR related issues, TSS also investigate matters relating to counterfeit goods, false descriptions applied to goods and services and misleading advertising. TSS can inspect trade premises in the local area to ensure compliance with these laws. Furthermore, the duties and responsibilities of the TSS extend well beyond the consumer protection matters we address here, to include, for example, product safety, food quality and animal health issues.

## Other enforcement agencies

8.9. Although our study principally focused on the role of OFT and TSS in the enforcement of the consumer protection regime, other parties have an interest in internet activities and issues that might influence consumer and business confidence in the internet environment. These individually hold a range of criminal and civil powers.

8.10. In terms of civil powers there are two types of enforcers specified under Part 8 of the EA2002:

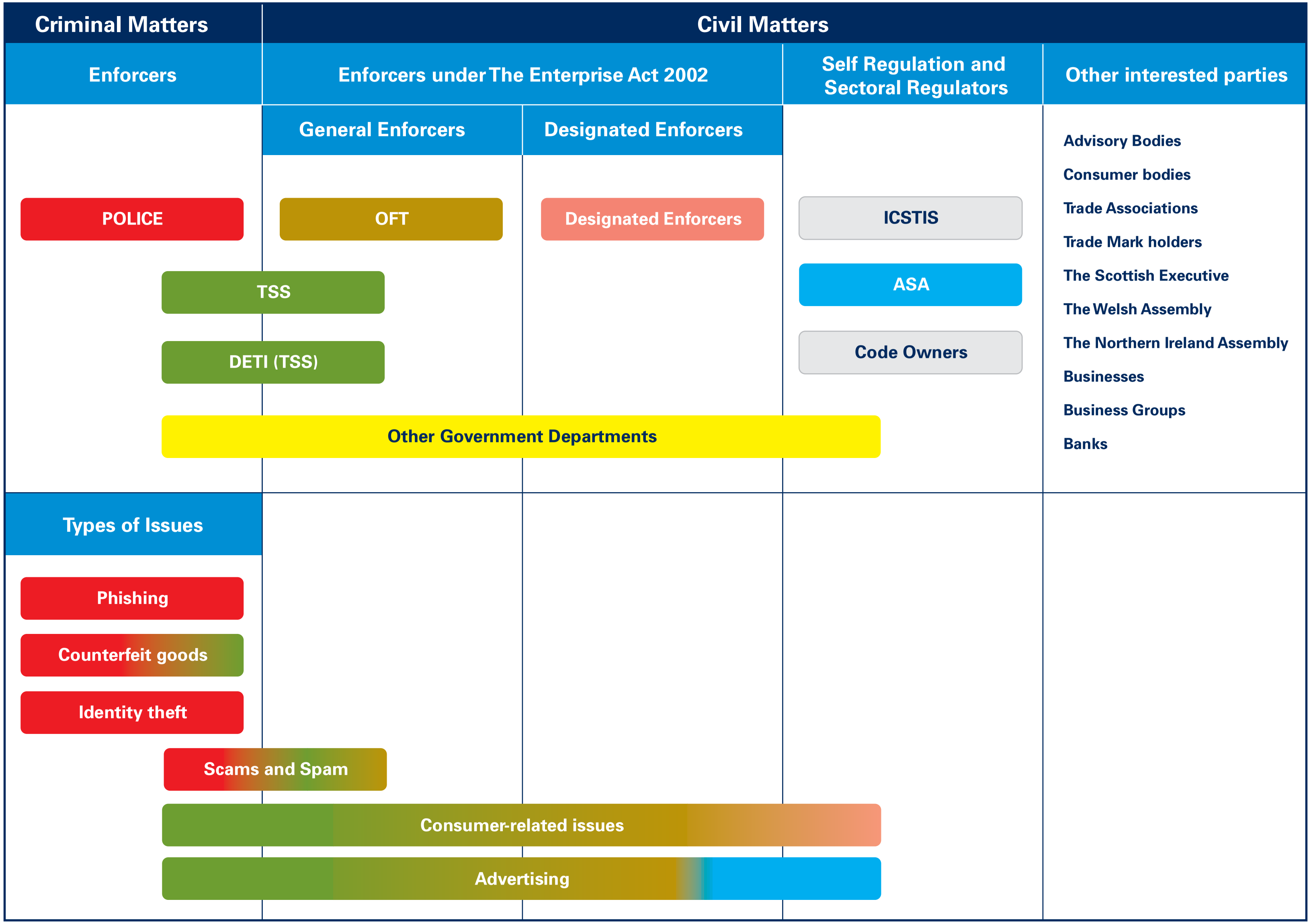
- General enforcers, who are the Office of Fair Trading (OFT), the Local Authority Trading Standards Services (TSS),[197] and the Department of Enterprise, Trade and Investment in Northern Ireland (DETI)
- Designated enforcers so designated by the Secretary of State[198]

8.11. Figure 8.1 is one way of depicting some of the key issues and range of enforcers and parties involved in protecting consumer and business interests on the internet. While the diagram is not a comprehensive representation, it illustrates the complexity of the medium and the potential range of parties with an interest in it.

[197] Additionally TSS also have enforcement powers for most consumer protection legislation outside EA2002.

[198] A designated enforcer is any person or body (whether or not incorporated) which the Secretary of State thinks has as one of its purposes the protection of collective interests of consumers and designates by order (Enterprise Act 2002 (Part 8 Designated Enforcers: Criteria For Designation, Designation Of Public Bodies As Designated Enforcers And Transitional Provisions) Order 2003/1399. See: www.opsi.gov.uk/si/si2003/20031399.htm. The designated enforcers are CAA, OFREG, Ofcom, OFWAT, OFGEM, ICO and ORR. The FSA, and Which? (formerly the Consumers' Association) were also designated under Enterprise Act (Part 8) (Designation of the Financial Services Authority as a Designated Enforcer) Order 2004, SI 2004/935, and Enterprise Act 2002 (Part 8) (Designation of the Consumers' Association) Order 2005, SI 2005/917.

Figure 8.1: Enforcement Framework



Criminal Matters

Civil Matters

Enforcers

Enforcers under The Enterprise Act 2002

Self Regulation and Sectoral Regulators

Other interested parties

General Enforcers

Designated Enforcers

POLICE

OFT

Designated Enforcers

ICSTIS

TSS

ASA

DETI (TSS)

Code Owners

Other Government Departments

Advisory Bodies

Consumer bodies

Trade Associations

Trade Mark holders

The Scottish Executive

The Welsh Assembly

The Northern Ireland Assembly

Businesses

Business Groups

Banks

Types of Issues

Phishing

Counterfeit goods

Identity theft

Scams and Spam

Consumer-related issues

Advertising

## Local prioritisation

8.12. TSS are therefore key players in the regulation of internet shopping. However, local authorities face many competing demands on their resources (some of them mandatory) and the internet is just one of numerous concerns for TSS. There is a reference to internet enforcement within the National Performance Framework, which is currently used as a basis to set TSS priorities,[199] however, there are no specific requirements on TSS relating to the internet – such as the level or type of enforcement they are expected to perform.

8.13. Officers we spoke to emphasised that their enforcement action was generally reactive to complaints, and that the issues faced by consumers and businesses was likely to differ between areas, as might consumers' knowledge about their rights and to whom they could complain.

8.14. The responses to our survey of TSS seemed to confirm that the level of priority given to the internet varied between TSS. Half (49 per cent) of the TSS responding said that they gave equal priority to ensuring compliance by both internet traders and High Street traders with the relevant regulations. The split between those who give internet traders higher priority and those who give lower priority was fairly even (27 per cent and 24 per cent respectively).

8.15. However, in discussions with stakeholders and at our workshop with enforcers, views were expressed that the internet might not be receiving the level of attention it warranted at a national or local level, specifically with regard to ensuring traders complied with the DSRs and the ECRs. One trade body felt that TSS were under-resourced and could not cope with issues arising from the expansion of the internet, while another commented that enforcement activity seemed to vary in intensity by region.

8.16. At our workshop of enforcers, there was general agreement that the internet deserved to be given more prominence. The view recorded, was that:

> *'…internet shopping needs to be higher up the agenda – there needs to be someone to give priority to the internet. Internet trading is a priority because we have not done much in this area: it is not that the internet is more important, it just needs more focus to bring it up to speed with other work.'*

## Current developments

8.17. Recent developments could have implications for TSS priorities, with the drive towards better prioritisation and improved cross boundary, regional and national working between TSS, and between the TSS and the OFT (see Chapter 12). Of crucial significance is the Regulatory Enforcement & Sanctions Bill,[200] which will establish the Local Better Regulation Office (LBRO) as a statutory body to encourage the implementation of a consistent and coordinated risk-based approach to enforcement and inspection at local authority level.

[199] See www.dti.gov.uk/consumers/enforcement/trading-standards/National%20Performance%20Framework/page24946.html The Performance Measures Guidance 2006/7 (see: www.dti.gov.uk/files/file38679.pdf) includes 'virtual inspections' within its measure of 'other enforcement activity' (this includes internet businesses, mail shots, mail order, and telesales).

[200] Further information can be found at: www.cabinetoffice.gov.uk/regulation/reform/hampton/latest.asp.

8.18. Also, in seeking greater consistency regarding enforcement priorities across the country, the Rogers Review[201] has identified six national enforcement priorities. These include the priority of fair trading which includes scams, rogue traders and intellectual property crime. The OFT and TSS will need to respond to these new agendas and work closely with LBRO to achieve greater consistency of outcomes, including in relation to online shopping.

8.19. A good starting point is to gauge the current situation with regard to enforcement activity for internet shopping, so below we consider the evidence on existing TSS compliance strategies and enforcement action.

## Enforcement and compliance activities

8.20. As we discussed in preceding Chapters, internet shopping is a rapidly growing feature of UK retailing. Some forecasts suggest sales could exceed 9 per cent of all retail spend by 2011.[202] As a result of this growth, internet purchases are increasingly likely to be a source of consumer problems and complaints.

8.21. Nearly a quarter (23 per cent) of internet shoppers had experienced at least one problem after buying online in the year to November 2006, and internet-related complaints received by Consumer Direct have grown to nearly 8 per cent of all their complaints, from 4.6 per cent in 2004. This trend is likely to continue as sales expand. Furthermore, our consumer survey found that 20 per cent of respondents who had experienced a problem purchasing over the internet did not secure satisfactory redress.

8.22. We therefore explore below what enforcers told us they were doing to help prevent problems arising, as well as what sorts of cases they were handling and how.

### Compliance strategies

8.23. In our survey of TSS and discussions with officers, we asked what proactive steps they took to ensure that businesses and consumers knew about consumers' rights when buying online, and to test whether businesses were complying. Very broadly, their activities included:

- Providing advice and guidance
- Monitoring and testing for compliance
- Investigations and prosecutions

#### Providing advice and guidance

8.24. At a national level, bodies with regulatory interests such as OFT, DTI and LACORS have issued guidance to businesses and consumers, either on internet shopping in general, or to address a specific market or area of concern. For instance:

- In May 2005, OFT issued guidance on cars sold over the internet. This was followed with guidance on IT consumer contracts sold at distance (Dec 2005), following an OFT study of this sector. [203]

[201] Further information can be found at: www.cabinetoffice.gov.uk/regulation/reviewing_regulation/rogers_review/index.asp.

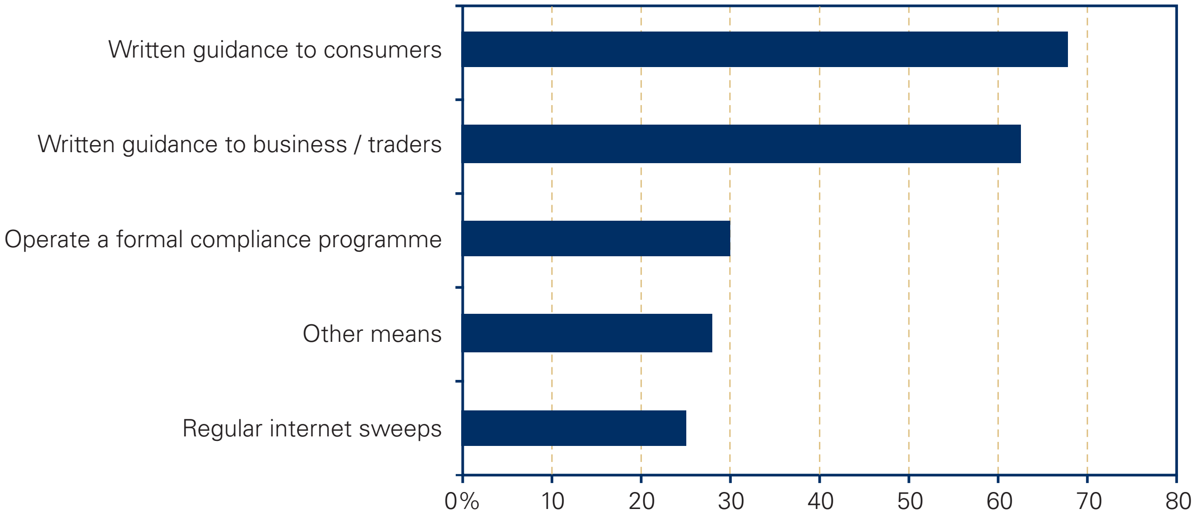
[202] Verdict (2007b).

[203] Available at www.oft.gov.uk.

- In May 2006, LACORS in consultation with IMRG issued model terms for internet retailers.[204]
- In September 2006 the OFT and the DTI jointly produced updated Guidance on DSRs. This provides a single and consistent source of information for businesses, their advisors and enforcers.[205]

8.25. We found that a significant number of TSS also provided written guidance on internet shopping: two thirds (67 per cent) published guidance for consumers; and 62 per cent published guidance for businesses (see Chart 8.1). We were told that businesses sometimes sought advice on 'what if' scenarios relating to specific problems to gain a better understanding of the regulations. TSS told us that the provision of advice and guidance by enforcers is a key tool in achieving compliance by traders and potentially more cost-effective than taking enforcement action.

**Chart 8.1: Internet purchases and rights; TSS action to address awareness and compliance**



Source: OFT TSS survey

8.26. However, despite these clear efforts by enforcers, we have found relatively low internet trader awareness of, and compliance with, the regulations, as well as weak consumer awareness (see Chapter 6 for more details).

8.27. In our TSS survey 93 per cent agreed or strongly agreed that more guidance was needed for businesses. Many enforcement stakeholders also commented that better guidance was needed for businesses and consumers – echoing the views of these groups themselves (see Chapter 6).

8.28. Our findings suggest that we need to look more closely at exactly what information is required and how it can be most effectively targeted at those traders and consumers who would particularly benefit from guidance.

[204] Available at: www.lacors.gov.uk/lacors/PressReleaseDetails.aspx?id=8.

[205] Available at www.oft.gov.uk.

## Monitoring and testing for compliance

8.29. The current enforcement structure is based on the traditional model of commerce where a business has a physical presence locally and is easily identifiable, and where the business usually has a local clientele. Also, under the Home Authority Principle (HAP) a business operating across the UK should be able to rely on a single local authority for regulatory advice and support.[206]

8.30. However, internet traders generally sell across local and regional boundaries and not all of them have a clear physical trading location. A TSS may therefore be unaware of which internet traders are based in their area. This view was expressed in the survey by one TSS:

*'…it is not possible to easily identify all businesses trading online from a particular geographical area. Time consuming searches, for example, under business type need to be carried out and there is no way of checking whether all the relevant businesses have been identified.'*

8.31. This then has implications for undertaking proactive work and as one TSS stated:

*'…Whilst it is easy to plan an inspection regime of High Street Shops and use Home Authorities to assist in ensuring compliance – there are major issues in deciding who should carry out proactive work on internet traders whose location is not known.'*

8.32. Despite these restrictions, we found that 30 per cent of those TSS who responded to our survey operate a formal compliance programme for internet traders based in their authority. We were told that these covered a number of initiatives, ranging from a programmed annual check of locally based web traders, to ensuring that the website of local offline traders were also checked and identifying and checking businesses on auction sites.

8.33. We also found evidence of the use of approaches specific to the internet such as web sweeps. Of those TSS responding to our survey, 25 per cent said that they undertook regular monitoring using internet sweeps. We found a number of examples of where web sweeps had been undertaken (Box 8.2).

8.34. These examples were part of wider campaigns that were well targeted and co-ordinated and which attracted publicity. As well as illustrating the breadth of issues faced by enforcers, the results of the web sweeps specific to the DSRs and ECRs[207] demonstrated a fair degree of non-compliance with the regulations by traders.

[206] For example, a multi-site retailer who seeks guidance from one local authority on product labelling, should feel assured that if the guidance is followed, it will not be challenged in any of its individual outlets by other local authorities. The Home Authority Principle (HAP) is currently being considered as part of the Regulatory Enforcement & Sanctions Bill as to whether it should be put on a statutory basis and referred to as the Primary Authority Principle (PAP).

[207] Evidence from OFT's website review for this Study can be found in Chapter 6.

### Box 8.2: Examples of web sweeps

Web sweeps are exercises in which enforcers identify and review websites to assess their compliance with a range of consumer protection legislation. They are often thematic, focusing on particular sectors or practices. Examples have included:

- In 2001, the OFT and 28 TSS worked with international consumer organisations to assess the quality of websites against international and domestic information requirements. Of the 637 sites examined in the UK, 52 per cent were non-compliant. These were followed up either directly with the business or by referral to the TSS where the business was based
- In 2002 the OFT, Medicine Controls Agency and 21 trading standards authorities worked alongside international partners searching for websites making potentially misleading claims about health products and 'miracle' cures. Over 170 UK-based websites were identified as potentially misleading during the sweep[208]
- The annual web-sweep organised by ICPEN, has also shown a high level of misleading advertising online. In 2004 an international sweep of the internet found 176 websites based in the UK that were making misleading claims.[209] In looking at these websites more than 234 breaches of consumer protection legislation were identified
- North Yorkshire Trading Standards, focusing in one web sweep on the sale of counterfeit goods online found 11,298 counterfeit video titles offered for sale by 269 individuals in towns and cities across the UK[210]

8.35. For web sweeps to be most effective, however, they need to be co-ordinated at a national level and targeted at a specific market sector or type of trader. In some regions, new arrangements have been introduced following the appointment of Regional Intelligence Officers[211] to better coordinate compliance and enforcement activities across a region. However, nearly nine in ten (89 per cent) of respondents to the TSS survey believed that cross regional work in relation to the internet should be strengthened.

8.36. This would seem to point to the potential value in developing some means of central identification of patterns of complaints and trends across the country. In part, this could be achieved through the improved use of national data that is available from Consumer Direct.[212] This would allow enforcers to assess the problems faced by consumers and indicate where resources should be focused.

8.37. The benefits of a co-ordinated approach to the internet could also be realised within the latest developments that are seeking greater consistency in the application of consumer protection nationally. For instance LBRO's core aim will be to support local authorities to regulate more effectively and more consistently, thereby reducing burdens on business.

[208] www.oft.gov.uk/news/press/2002/14-02#.

[209] The OFT and 30 TSS plus 24 enforcement agencies in 31 countries surfing the internet for websites that make misleading claims, as part of ICPEN's sweep. A total of 1847 sites were identified worldwide (OFT PN 61/04). See www.oft.gov.uk/news/press/2004/61-04.

[210] See: www.tsi.org.uk/media/index.htm?frmClient=8AA37B84-1185-6B25-FC2C8AD741D101F2&frmItemID=167768& frmShared=1.

[211] The DTI is funding a regional intelligence capability to facilitate better intelligence-led enforcement and improve cross-boundary enforcement, in 2006-7 and 2007-8. Currently, Consumer Direct forward complaints to both the consumer's and trader's TSS. Complaints can be referred or notified. A referral requires action by the TSS and a notification is for information only.

[212] Currently, Consumer Direct forward complaints to both the consumer's and trader's TSS. Complaints can be referred or notified. A referral requires action by the TSS and a notification is for information only.

8.38. We also found evidence of the use of test purchases in relation to online shopping.[213] Sixteen per cent of TSS responding to our survey indicated that they often made test purchases and 41 per cent said that they did so sometimes. A number of Trading Standing Officers told us that test purchases can also be a useful investigatory tool – indeed, they can be vital in obtaining evidence to support a prosecution, for example for the sale of counterfeit goods.

8.39. We found examples of test purchases being used to verify civil obligations (for example, provision of durable information, cancellation rights) and the overall selling experience, before an approach by the TSS was made to the trader based in its area.

8.40. However, to conduct online test purchases, certain resources are ideally required; such as a stand-alone PC, a budget to purchase goods, an unidentifiable credit card account to make purchases and a residential location for deliveries. Respondents to our survey and in our workshop commented that these resources were not always provided by all TSS departments, potentially limiting the application of this tool. And where resources were provided, some said that local policies may impose constraints on how they could be used.

## Investigations and prosecutions

### OFT cases

8.41. Since the implementation of the DSRs, the OFT has challenged or provided advice on a number of specific practices that it considered infringed the regulations.[214] For example, the OFT advised businesses that they could not make the right to cancel conditional on the goods being returned unopened or in their original packaging, where such conditions restricted consumers' ability to examine goods under the DSRs.

8.42. However, there can sometimes be risks in taking action as illustrated by the case study in Box 8.3, in which the European Court eventually ruled in favour of the company. Nevertheless, this court action did clarify the law on the applicability of cancellation rights in this sector.

### Box 8.3: Case study – cancellation rights for self drive car hire contracts

In 2001, following consumer complaints OFT approached easyCar believing it to be in breach of the DSRs by refusing to give cancellation rights to consumers entering into self drive car hire contracts over the Internet. easyCar's view was that the hire contracts which it offers were covered by the exemption laid down for 'contracts for the provision of … transport … services' within the meaning of Regulation 6(2) of the DSRs and Article 3(2) of the Directive, and, therefore, exempt from the cancellation provisions in the DSRs. The OFT, however, contended that car hire cannot be characterised as a 'transport service'.

Following a hearing in the High Court, the matter was referred to the European Court who ruled in favour of easyCar.[215] The court held that the partial exemption to the DSRs for 'contracts for the provision of …. Transport … services' included self drive car hire.

[213] Test purchases on the internet are usually triggered by a high number of complaints against a trader in the TSS area. They may involve ordering products online and testing whether problems are encountered with delivery or cancellations. They may be used to gather evidence for a criminal prosecution, or to check the safety of a product, particularly imports, which may not comply with UK safety regulations.

[214] Amazon and BOL agree to refund delivery charges: www.oft.gov.uk/news/press/2002/pn_33-02; Virgin Wine give consumers fairer online deal: www.oft.gov.uk/news/press/2003/pn_58-03; Computer companies warned over unfair contracts and sales methods: www.oft.gov.uk/news/press/2003/pn_77-03. Dell to improve terms and conditions for consumers: www.oft.gov.uk/news/press/2006/111-06; Internet car dealers give undertakings to the OFT: www.oft.gov.uk/news/press/2006/142-06; Computer companies warned over unfair contracts and sales methods: www.oft.gov.uk/news/press/2003/pn_77-03.

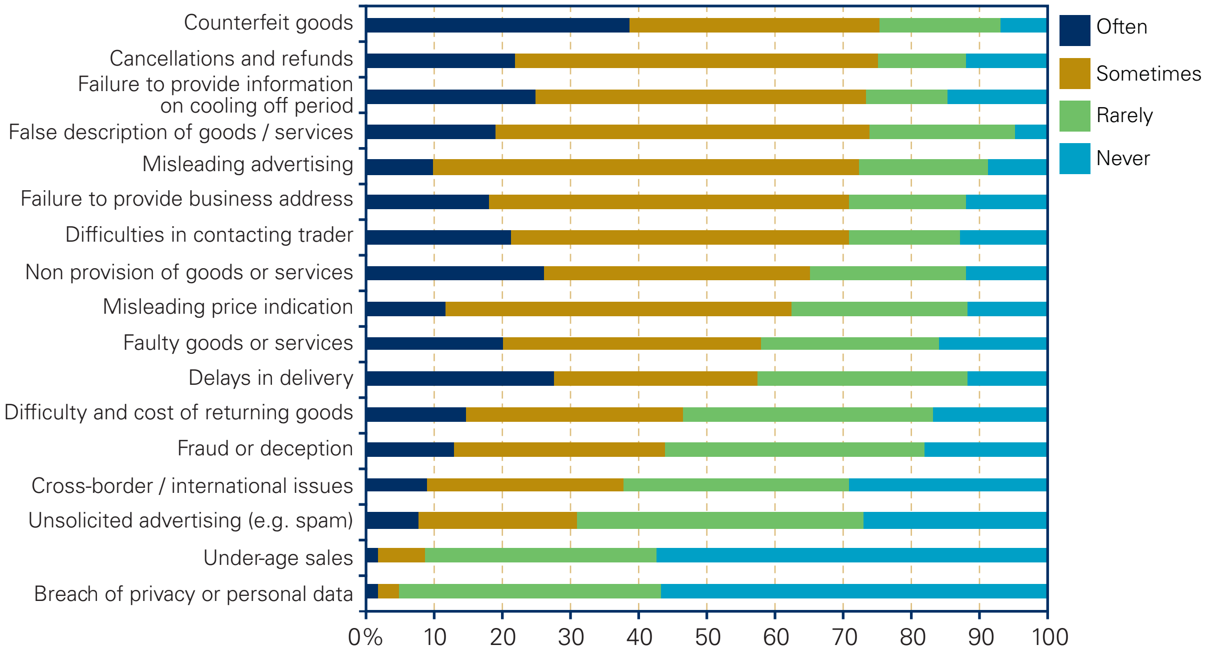
[215] See: curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&Submit=Submit&docrequire=alldocs&numaff=C-336%2F03&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100.

## TSS Investigations

8.43. While the web sweeps listed in Box 8.2 above illustrated the breadth of the issues faced by enforcers on the internet, TSS responding to our survey told us that the main problems they had investigated in 2005 had related to counterfeit goods, cancellations and refunds (see Chart 8.2). Failure to provide information on the cooling off period, false description of goods/services, misleading advertising, failure to provide business address and difficulties in contacting trader were also relatively frequent issues. Breach of privacy or personal data and under-age sales were least likely to be investigated.

8.44. Broadly it appears that enforcers are addressing the main distance selling issues that prove to be most problematic for consumers (see Chapter 5) – including delivery, problems communicating with traders, non-provision of goods or services, difficulties with refunds and returns, and misleading claims.[216]

**Chart 8.2: Issues addressed in TSS internet sales-related investigations (2005)**



Source: OFT TSS survey

8.45. The attention paid to counterfeiting appears proportionately greater than its profile in terms of the number of problems consumers claimed to have experienced (other than in relation to users of auctions). However, it was suggested to us that there may be a number of reasons for this. For instance, some consumers may not know that they have bought a counterfeit or they may knowingly buy counterfeit goods. Additionally trade mark holders may be raising

[216] Our consumer survey found that 48 per cent of those who had experienced a problem shopping online in the past 12 months said the most recent problem related to delivery. The second most frequently mentioned problems related to problems communicating with the trader (14 per cent). However, when combined, wrong, damaged, faulty or poor quality goods were also a typical cause of complaint, accounting for 17 per cent of the problems most recently experienced. Likewise, when combined, difficulties with refunds and returns accounted for 16 per cent of problems consumers said they had experienced. Consumers also told us that they had concerns about being misled – for instance, 83 per cent of telephone survey respondents were bothered that some sites advertised products at a certain price and then added on unexpected additional charges.

awareness of counterfeit products on the internet with TSS; and TSS, as part of their inspection duties, may be increasingly identifying counterfeit products on the internet. The emphasis on combating the sale of counterfeit goods online is likely to continue following the Gowers Review, which recommends that additional funds are provided to TSS to combat infringements of copyright law.[217]

## TSS Investigations – actions taken

8.46. We asked TSS in our survey to provide a figure for the number of investigations they had launched in 2005 relating to internet sales. Approximately half of the respondents (52 per cent) gave a figure, and more than half of these responses were based on estimates rather than on hard data. Therefore, the median response of six per cent of all cases being related to internet shopping must be treated with care.

8.47. There was, however, some evidence to support the contention reported at paragraph 8.13 above that the proportion of internet related cases varied quite considerably across authorities (from zero to 57 per cent).

8.48. As we noted above, enforcers have limited resources to respond to a broad range of problems and each TSS will act according to what they see as their priorities at the local level. They will also consider a range of options in terms of how they respond to breaches in legislation. For example, they could provide advice and guidance to the business, issue a warning, or initiate a civil or criminal investigation or both. There is, therefore, discretion as to the choice of option, although that discretion is subject to general administrative law principles and the guiding principles set out in the Cabinet Office enforcement concordat.[218]

8.49. Our TSS survey found that in cases relating to internet trading, criminal enforcement powers were most often used: 76 per cent of respondents stated that criminal enforcement powers were ‘often’ or ‘sometimes’ used in cases relating to internet trading, only 21 per cent had ‘sometimes’ or ‘often’ used the civil investigative mechanisms under the EA2002.

8.50. This suggests that enforcement activity is being targeted against businesses engaged in activities that breach criminal law, reflecting TSS priorities of where consumer detriment is seen to be greatest. Additionally, the use of criminal powers is often seen by TSS as the most effective way to bring an illegal practice to an end.

8.51. There may be other reasons why criminal enforcement powers are used as often as they are in relation to internet-based investigations and from talking to a number of TSS it became clear that TSS expertise lies in undertaking criminal cases.

[217] See: Gowers (2006).

[218] Available at www.cabinetoffice.gov.uk. In addition, the Cabinet Office is currently consulting on a Regulators’ Compliance Code (see: www.cabinetoffice.gov.uk/regulation/consultation/current/index.asp.) that will require regulators to have regard to the Code when determining policies, setting standards or giving guidance in relation to the exercise of these functions. As such, the Code applies to the general level functions, such as policy making and standard setting and not directly to individual level functions of carrying out inspections, investigations, prosecution and other enforcement activities.

8.52. However, this situation has implications for internet shopping as the DSRs (in the main)[219] and the ECRs, are ultimately enforced in the civil courts. If resources have tended to be targeted at priorities that require the cessation of criminal activities rather than compliance with the DSRs and ECRs, this could in part explain why some stakeholders perceived a lack of action.

8.53. Some respondents to the TSS survey suggested that criminal sanctions should be applied to a wider range of offences under the DSRs. Whilst the Directive allows for member states to introduce more stringent provisions into their domestic legislation to provide a higher level of consumer protection than that referred to in the Directive, this would require a review by the DTI and needs to be considered in the wider context of the Macrory review of penalties discussed below at paragraph 8.55.

8.54. The general use of criminal rather than civil powers was echoed in an independent evaluation[220] of OFT training provided to TSS in the use of the EA2002. This found that while TSS knowledge of and confidence in the use of civil powers had increased substantially,[221] more training, and support was needed to address knowledge and confidence issues that may hinder the wider use of the EA2002. The report identified a continuing role for OFT to ensure greater consistency in the use and effectiveness of the EA2002 as an enforcement tool.

## A flexible, proportionate and targeted approach

8.55. This discussion regarding the use of powers by enforcers against internet traders needs to be placed in the wider context of the Macrory Report.[222] The report, published in November 2006 recognised the importance for enforcers and regulators having a flexible and proportionate sanctioning toolkit. Amongst other things, it suggested enforcers publish an enforcement policy and raised the prospect of traders receiving an administrative penalty as an alternative to criminal prosecutions.[223] The draft Regulatory Enforcement & Sanctions Bill includes the key recommendations from the Macrory Report.[224]

8.56. The recommendations address the way enforcement is currently carried out and, if adopted, will have implications for enforcement of traders generally, including internet traders. The aim is to provide a broad range of regulatory sanctions to allow regulators to select the most appropriate and effective response to a particular instance of regulatory non-compliance.

8.57. Currently, there is no national strategy regarding what remedies should be used in relation to traders on the internet. However, in keeping with the tailored approach embodied in the Macrory Report, many TSS we spoke to suggested that there was a range of traders and circumstances, requiring different responses in order to achieve compliance. This could help to ensure that resources are targeted to where consumer detriment is greatest.

[219] The DSRs do have criminal sanctions where suppliers demand payments for unsolicited goods and services (regulation 24) www.opsi.gov.uk/si/si2000/20002334.htm.

[220] www.oft.gov.uk/news/press/2006/176-06. Evaluation of Enterprise Act training for TSS (December 2006) paragraphs 1.9 to 1.15.

[221] Over 40 per cent of TSS have now undertaken the EA2002 Training provided by OFT.

[222] Macrory (2006).

[223] Macrory (2006) refers to the undertaking and undertakings Plus (a combination of an Enforceable Undertaking with an administrative fine) www.cabinetoffice.gov.uk/regulation/reviewing_regulation/penalties/

[224] Further information can be found at: www.cabinetoffice.gov.uk/regulation/reform/hampton/latest.asp

8.58. The internet is arguably having an impact on the overall structure of the retail market. Within this evolving environment, there is a diverse range of traders. These include well known High Street names who have established a presence on the web; small independent businesses increasing their exposure to a potentially wider clientele, and individuals potentially engaging in what may be considered commercial activities, for example via auction sites. As a result, we identified four broad categories of 'seller' on the internet (see Box 8.4).

8.59. This has important implications for enforcement. As one officer responding to our survey, told us: *'Internet investigations include national retailers, very small independents and auction sellers. Each requires a different approach and each poses its own problems.'*

### Box 8.4: Enforcement – a typology of online sellers

We identified four broad categories of 'seller' on the internet:

**Type 1:** traders who had good knowledge of regulatory requirements and good levels of compliance. They may have access to in-house legal advice, be members of a Trade Association or code scheme.

**Type 2:** traders who have good knowledge of regulatory requirements but, for whatever reasons, lower levels of compliance.

**Type 3:** traders with poor knowledge and poor compliance, but who are likely to comply if approached.

**Type 4:** 'rogue traders', who irrespective of the awareness and knowledge of the regulations have no intention of complying with them.

8.60. Broadly speaking, this range of 'sellers' is likely to attract differing responses from enforcers. Traders falling in the first category may need a light touch approach, including advising them on new regulatory developments. Those in Category 2 and 3 may need a firm guiding hand, with the threat of enforcement action where necessary. In seeking compliance by traders falling in categories 2 and 3, enforcers have a mix of tools available to them ranging from provision of advice to enforcement action, both civil and criminal. At the far end of the spectrum, businesses with little or no intention of complying present the greatest problem, not only because they sometimes fall into the category of traders who are difficult to track but also because swift enforcement action is often required to address their behaviour.

8.61. An area for further consideration could therefore be a clearer formulation of how best to target enforcement activity and, where needed, enforcement action for internet shopping according to the greatest risk and detriment for consumers.

## The internet – challenges for enforcers

8.62. Our survey of TSS and discussions with officers also identified that the internet can raise particular challenges. Frequently mentioned issues included the difficulties in tracing site owners, and the rapid pace of change with its implications for their skill set and access to specialist software and internet investigative tools.

### Anonymity and the ability to trace website owners

8.63. It is likely that when consumers complain to their local TSS about an online trader, they may be complaining about a business based in another authority, region or even country. This means that TSS spend resources on identifying where the trader is based.

8.64. While we found examples where tracing the location of a rogue trader was a particular problem, we also found examples of a lack of compliance with DSRs and ECRs by 'legitimate' traders who had not provided a contact address on their website.[225] Further details regarding compliance can be found in Chapter 6, including the outcomes of our websites review. The case studies in Box 8.5 illustrate the difficulties faced by consumers when purchasing online from a trader who has not provided a contact address.

8.65. In trying to track down the location of internet traders, enforcers can use a domain name registrants free online search facility, called 'WHOIS'[226] (see the second example in Box 8.5). This enables an enquirer to find out whether a domain name is available and, if not, the organisation or person to whom it is registered, and when that registration was made.

**Box 8.5: Case studies – tracing website owners**

#### Case study one:

Mrs S bought an item from a .co.uk website, thinking she was buying from a UK company. The goods were faulty and she discovered that there was no return address on the website. She contacted the trader by email who was unwilling to accept the goods back. On advice from her local trading standards service she sought and received a full refund from her credit card company. She was then harassed by emails from the company demanding their goods back although they still did not provide a return address causing considerable distress. It is believed that the business was located in Hong Kong.

#### Case study two:

TSS received a complaint from a local business concerning a trader setting up a fraudulent website, using the local trader's address details. The website concerned was offering high value items such as jet-skis, motorbikes, quads, tractors etc. The only way to pay was by bank transfer or credit/debit cards.

The address for the trader shown on the website changed four times, and two of the addresses shown were entirely fictitious. WHOIS information for the website gave a name and address in the USA. The bank details were however traced to Spain.

The case came to the TSS attention twice. Originally trading with a .com tag (which was successfully shut down), the same scam then appeared on a similar named website with a .org tag

[225] For example, during 2006, Consumer Direct, under the category 'Internet' logged 864 calls which had no trader details and for 'Internet Auctions', the figure was 171.

[226] WHOIS can only search for domain name registrations ending in co.uk. ltd.uk, me.uk, net.uk, org.uk, plc.uk, and sch.uk. For other domain name endings such as .org, .com, other WHOIS databases can be interrogated. Most, if not all, Top Level Domain registries provide a WHOIS service, with varying types of data available e.g. phone, fax, email address.

8.66. While WHOIS is a useful research tool, it can have some limitations. For instance, an individual not acting in the course of a business can ask that the address be withheld from the public domain. Nominet, who control the '.uk' top level domain name and receives an average of 6,000 registrations a day, told us that it would be impractical to verify details on all applications and that it therefore relies heavily on the integrity of the registrant to provide accurate information in the first place. However, Nominet also said that if it becomes aware that false contact information has been provided, it takes action to delete the relevant domain name registration. Nominet also said that it would disclose opted out WHOIS data to enforcers provided they could demonstrate a legitimate reason for requesting the data. This is a potentially valuable facility for TSS.

8.67. Stakeholders in the industry told us that while the internet appeared to enable anonymity on first examination, it can, in fact, be a potential tool in investigations since 'footprints' were invariably left by its users. Therefore, in addition to the formal powers of investigation, for example offered under the use of RIPA[227] powers, there is an opportunity for closer informal working with internet gatekeepers who hold information on traders, such as Nominet and the ISPs, subject to any constraints under the law. We found some good examples of TSS and ISPs working together to identify and either temporarily suspend or take down problematic websites.[228] This suggests that there is potential value in investigating a common national level framework for cooperation with members of the industry.

8.68. Although the value of international trading remains at a relatively modest level (see Chapter 11), enforcers noted that they often found that problem traders and rogues were based overseas. Enforcers claimed that this raised particular difficulties in contacting and communicating with traders, as well as jurisdictional uncertainties (see Chapter 11). At our workshop, it was clear that there was uncertainty about how cases involving other countries should be handled. Several attendees pointed out that better communication and co-ordination was needed between the OFT and TSS on international cross-border cases.

### The dynamic nature of the internet

8.69. The internet is a fast changing environment, with new hardware and software emerging at a rapid pace and new market models evolving (discussed further in Chapter 12). While the core analytical skills for investigating internet traders are not dissimilar to what may be found in other enforcement work, our survey revealed that there was an equal split between those who thought that they had the necessary skills to investigate online traders and those who did not.

8.70. Although funding has been provided in recent years for the training of enforcers on e-commerce investigations[229] it was not part of an on-going programme. To keep pace with the developments of the internet, such knowledge needs to be maintained through continual use and updating. However, as TSS face competing priorities, some workshop attendees questioned whether there would ever be enough cases at a local level for officers to develop and maintain a sufficient level of knowledge and skills. This led to a suggestion for a central

[227] Regulation of Investigatory Powers Act 2000 www.opsi.gov.uk/Acts/acts2000/20000023.htm.

[228] A TSS provided examples of requests sent to Internet Service Providers to remove websites where there was evidence of criminal activity.

[229] DTI Millennium Fund allocated to e-commerce work. A project that won DTI funding was proposed by SETSA (South East Trading Standards Authorities) in partnership with TSI. The project aimed to improve, nationally, TSS ability to give quality, proactive advice and reactive enforcement on e-commerce and cybercrime issues. Three types of training courses were provided which covered, enforcement on the internet (investigating complaints and offences), digital evidence (seizing, transporting and storing digital evidence within a criminal investigation) and e-commerce for business advisers (how to advise and assist traders on e-commerce matters including both criminal and civil topics).

resource and a network of regionally based 'expert' enforcers and mirrors comments provided in our survey of TSS, where there were suggestions for: *'specialist units…or an on-call expert helpdesk or regional expert, who would be available to visit any TSS to train/assist in any enquiry.'*

8.71. To assist local enforcement staff there has been the development of some resources to support internet investigations, such as the 'tool-kit' developed by the London Trading Standards Authorities (LoTSA). TSS are also supported by two Internet and computer crime 'Internet Labs'. The OFT also set up an 'Internet Lab' in October 2004 consisting of stand-alone PCs, removable hard disk drives and software that can take digital images of web pages, identify who may be behind an IP address and track the location of servers. This facility represents a useful resource which could be developed and used more for investigations and research on the internet.

8.72. We found that, although there are examples of expertise and specialist resource in relation to the internet, there was no consistency across the country. As a result, we suggest that enforcement in general and specifically DSR compliance of traders could be improved through specific training that reinforces a national strategy of compliance and enforcement. The potential benefits and cost-effectiveness of such an approach could be considered in any follow-up work.

8.73. Finally, significant developments such as targeted advertising, the convergence of platforms and even the growth of virtual worlds (see Chapter 12) could have important implications for enforcers. In addition, new search technologies and other IT tools may assist enforcers in the future. Despite the rapid pace of technological change, however, we came across no examples of significant foresight work on the part of central or local enforcers or with third parties involved in developing emerging technologies.

## Examples from other countries

8.74. In considering the domestic approach to enforcement of online consumer protection, we considered experiences in some other countries. While not a full analysis of all the pros and cons of different approaches, this did appear to offer useful insights and possible lessons (see Box 8.6).

8.75. In particular, we noted that the French and Belgians, having recognised the potential impact of the internet have established specialist national facilities that specifically monitor and investigate internet traders. The Japanese have adopted a 'customer watchdog' approach.

### Box 8.6: Enforcement lessons from some selected countries

- **France:** The DGCCRF (General Directorate for Competition, Consumer Affairs and Fraud Control) in France have created a small specialist unit, the Centre for E-Commerce Surveillance (CSCE), consisting of seven people, who support a network of 55 other staff located at the DGCCRF's regional offices around the country. The CSCE staff work full-time on internet issues and, amongst other referrals, receive all internet-shopping enquiries and complaints nationally. In response to these, they coordinate enforcement activity which is carried out by local enforcers in the department in which a particular trader is based. The regional staff handle offline as well as online enforcement, but they have particular responsibility for enforcement against internet traders in their own areas, as well as for surveillance in a particular sector of online business. This enables sectoral expertise to be built up, ensures clarity about responsibility, and prevents duplication of work. A check for regulatory compliance is also carried out on every new retail website using a standardised compliance checklist. The DGCCRF does not have particular powers for online surveillance or enforcement, and all the tools it uses in its surveillance activities are freely available on the web.

- **Belgium:** Belgium's DG Enforcement and Mediation contains a 'cell' for Internet Surveillance, which employs five staff working full-time on e-commerce related matters. The team constantly monitors websites on its own initiative and in response to consumer complaints. The cell functions both as a centre for expertise on internet research and enforcement, and as a basis to introduce these techniques into the daily work of every enforcement agent. This body also cooperates closely with the Federal Computer Crime unit of the Federal Police, on a common online complaint form and database called E-cops. The cell for Internet Surveillance units has adopted a system of 'informative emails': when it establishes infringements against Belgian law on websites, the companies first get an email informing them of the existing law and are given the chance to put the website in order within a certain time frame. If the trader continues to infringe the law, they receive an official report which eventually might lead to legal procedures. A direct approach such as this may be an effective means of: (a) communicating a clear message about a specific piece of relevant law; and (b) simultaneously addressing specific problems causing infringements.

- **Japan:** The Japan Fair Trade Commission (JFTC) has designated 80 consumers as 'Electronic Commercial Transaction Researchers'. These individuals are asked to monitor online advertising, and information they collect is used to increase compliance. The JFTC has the power to impose 'cease and desist' orders, which can be applied online and offline.

- **USA:** The Federal Trade Commission (FTC) is the OFT's US counterpart, responsible for competition and consumer regulation, and is involved in the incidence of, and protecting consumers from, online fraud. The FTC encourages consumers to file complaints to them, many of which are entered into the Consumer Sentinel Database – a secure online database available to more than 1500 civil and criminal law enforcement agencies in the United States and abroad. More than 150 other foreign and domestic government agencies and organisations also enter complaints into the database, to which more than a million entries were added in the 2005 fiscal year. Law enforcement agencies use this information to bring enforcement action. The three main areas on which the FTC's online consumer enforcement focuses are fraud, spam and spyware. The FTC also has an Internet Lab, used by agency staff to conduct law enforcement investigations. The lab provides FTC lawyers and investigators with hi-tech tools to investigate hi-tech consumer problems. It allows investigators to search for fraud and deception on the internet in a secure environment. To capture websites that come and go quickly, the lab also provides FTC staff with the necessary equipment to preserve evidence for presentation in court.

## Conclusions

8.76. In conclusion, we found examples of good practice and promising examples of proactive work, although the picture varied across the country. Actual enforcement of consumer protection, such as DSRs and ECRs online, could be more effective if it formed part of a national risk-based approach. This is because with differing priorities and resources, enforcement agencies will act differently in enforcing consumer protection legislation online. This may be exacerbated by a lack of specific training and sources of support provided to enforcement officers, as well as a lack of a strategic, long term approach to ensuring that enforcement agencies keep pace with technological developments.

## Next steps

8.77. In line with the principles of a targeted, risk-based approach, currently being established for enforcers, an issue for further consideration could be how best to target enforcement activity and, where needed, action, for internet shopping according to the greatest need. We also identified possible improvements to enforcement for internet shopping that warrant further exploration, including:

- Closer working between enforcers and industry players who may be able to help in identifying and tracing website owners, subject to any constraints under the law
- Developing technical expertise and awareness, by the pooling of skills in centres of expertise
- The provision of foresight work and partnership working with private sector players that are developing emerging technologies to assist enforcers with new tools and techniques
- The provision of greater central support or co-ordination to identify national patterns so that the current enforcement model, with its emphasis on local enforcement, could be most effectively applied to the internet in non-compliance. Other more active monitoring and surveillance approaches, such as that in France and Belgium, might be considered
- Increasing the uptake of the use of civil tools by the TSS to enforce the DSRs in relation to the internet. The OFT is currently working with TSS to provide training in the use of civil legislation under the Enterprise Act, which is being expanded to train local authority legal teams
- Improving communication and co-ordination between the key agencies to avoid any danger of issues falling between enforcers.

# 9 CONSUMER CHOICE IN ONLINE SHOPPING

## Summary

The internet has enabled businesses to establish a new means of selling by setting up their own websites, and adopting new business models to widen their reach. However, the vast range of retailers and offers available to shoppers can make it hard for them to locate and differentiate between competitors. We identified some significant differences in prices being charged for similar goods online – by an average of 30 to 60 per cent of the lowest price for music and electrical items we looked at. Fortunately, provided they are used well, tools such as search engines and price comparison sites can help consumers to make informed choices and save money.

However, we found that some consumers could benefit from searching more effectively online, particularly given limits to the numbers and range of traders listed by some price comparison sites. For instance, if a shopper used only one of ten price comparison sites, they had a 50 per cent chance of finding one of the lowest prices. We estimate that online shoppers who do not use search tools as well as they might and therefore limit their search, could miss out on potential savings of £150 million to £240 million per year.

We also found that in many cases, final prices differed from that first shown. For instance, for 47 per cent of the flights we looked at the price was higher. For these, the median price increase was 19 per cent, but some increases were much more. For online sales as a whole, we estimate that 1.2 million internet shoppers were unaware of these charges during the buying process, but still went on with their purchase and paid £60 million to £100 million each year as a result. Furthermore, in the sectors we looked at, there were examples of unclear information being presented. The laws are changing in this area to introduce a general duty not to trade unfairly. There could also be scope to improve the quality of information provided to consumers by extending advertising self-regulation to websites.

## Next steps

It is important that consumers appreciate the limitations of search sites and use them as effectively as possible. We will develop ways to raise awareness of how shoppers can make best use of the tools available to them. We will also explore with the Committee of Advertising Practice whether their remit could be extended to cover websites. Our planned work on raising awareness will include making clear to businesses their obligations when presenting information to consumers.

## Introduction

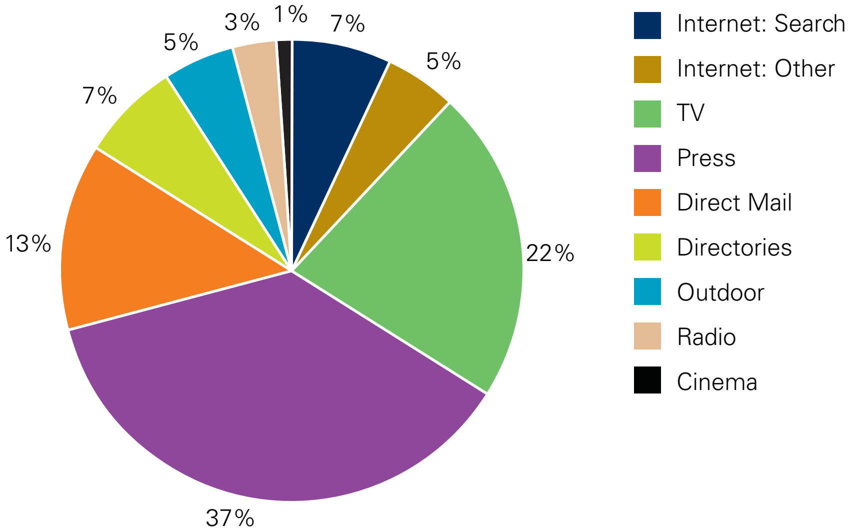
9.1. This chapter explores how consumers use the internet to find retailers, and look for products to buy. It considers the role of search intermediaries (search engines and price comparison sites) in this process, as well as whether consumers are able to make informed choices online. Before addressing how consumers choose online, however, we briefly consider the ways by which businesses sell to them.

## Attracting consumers: Websites and advertising

9.2. Many factors can determine whether a business website succeeds, including its ease of use and accessibility. However, one critical factor is the profile of the site and how easily consumers can find, or be directed, to it. With over 100 million websites in existence by 2007, search intermediaries play a critical role in connecting consumers and businesses. These intermediaries, such as dedicated search engines or sites that offer content (such as news and other information), or social networking sites are a popular business model. They are generally funded by advertising.

9.3. Online advertising is growing rapidly, and has become a significant way in which businesses can reach consumers. Total online advertising spend reached £2 billion[230] in 2006, having grown by 42 per cent on the previous year. It accounted for over 11 per cent of total UK advertising spend – more than cinema, outdoor and radio advertising combined.

**Chart 9.1: Market share of total £17.6bn UK advertising market in 2006[231]**



Source: PWC/IAB (2006)

9.4. Almost three fifths of the online total (58 per cent)[232] was accounted for by 'search advertising', such as paid for listings or prominence, which consumers are shown when they use search engines and price comparison sites. Paying to be displayed more prominently by these search intermediaries is an important part of establishing an online profile for many businesses. We found that 14 per cent of businesses that sell online pay to have their products featured more prominently on price comparison sites, while 34 per cent pay to be featured more prominently on search engines.

[230] All figures from PWC/IAB (2006).

[231] All figures from PWC/IAB (2006).

[232] Other online advertising: display (23 per cent), classifieds (19 per cent) and solus (1 per cent).

## Search engines and price comparison sites

9.5. Search engines and price comparison sites are both types of search intermediary unique to the internet that can empower consumers by enabling them to make more informed decisions. Provided they are comprehensive and reliable, and consumers use them well, they provide significant benefits by increasing the speed and effectiveness of search.

9.6. There is some evidence that search intermediaries can have important market effects. Although it is difficult to measure, one economic paper has found that the ease of search online has reduced prices online. Brown and Goolsbee's (2000) study of US life insurance prices in the 1990s concluded that for those categories where online search, such as via price comparison sites, was possible, prices were 8-15 per cent lower than they would have been without such a facility.

### Search engines

9.7. A search engine helps consumers find information on the internet. Examples include Google, Ask, Yahoo and MS Live Search.[233] Using key words relevant to what is being sought, the search engine retrieves and presents a list of references that match or include those words. They use an automated web browser (a 'spider') to follow and record links and create an index of pages. When a user requests a search, they are presented with a list of pages taken from the index containing their key words.

9.8. Most search engines assess the relevance of the indexed pages to the consumer's key words and present the sites in relevancy order. Engines differ in their method of ranking sites, but a common way to establish relevancy is to count the number of times a website is referred, or linked to, across the web. This assumes that a highly referenced website is relatively reliable or popular because it is useful.

9.9. Businesses can pay to advertise on search engines and reach the appropriate audience of consumers as they type in particular search terms. The main types of advertising that search engines offer are:

- **Paid for inclusion** – the retailer pays to be included on the search results
- **Paid for prominence** – the retailer pays to appear more prominently (higher up or with logo and other information) on the results page

9.10. Although retailers may pay to be included in the search engine's index ('Paid for Inclusion'), most search engines state that this does not affect prominence and is a convenient way for businesses to ensure that their site is covered immediately, when it might take an automated web browser much longer to find it.

9.11. In contrast 'Paid for Prominence' guarantees a retailer a high ranking, usually in relation to relevant words. These listings are usually segregated from the standard results and may be labelled to highlight that they are adverts. How clear and proximate the labels are is important to ensure consumers appreciate that they are adverts.

[233] According to www.hitwise.co.uk the most popular search engines in the UK in the four weeks ending 03/03/07 by volume of searches were Google with 78 per cent, yahoo with six per cent, ask with five per cent and msn with four per cent.

9.12. There are three major paid-for search advertising organisations, Google AdWords, Yahoo Search Marketing, and Microsoft adCenter,[234] some of which syndicate adverts to partner websites. Generally, they allow firms to bid on key words for which their website links will appear when a consumer's search inquiry includes that word. The firm's ranking in the paid for results can depend on factors such as the amount bid, as well as the volume of 'click throughs' their site receives. Over £1 billion was spent on 'search advertising' in the UK in 2006.[235] The importance of search is also underlined by the search engine optimisation (SEO) industry which is rapidly developing to help firms make their sites easily findable.

### Price comparison sites

9.13. Price, or product, comparison sites allow consumers to compare and contrast information on products sold by multiple firms on the same webpage. Examples include Kelkoo, Pricerunner, Shopping.com and Froogle.

9.14. Comparison sites typically direct customers to their listed retailers, and most limit their indices to retailers that pay to be listed. Retailers may also pay more to be listed higher up the results page or more prominently. They help consumers to select retailers and products by offering comparative price, delivery and sometimes stock information too. Many also present other information, such as shopping guides, third party reviews and consumer comments on the retailers and products. This kind of detail is not provided by general search engines and it might be time consuming for consumers to find similar information on numerous retailer websites.

## How well do consumers search online?

9.15. How consumers search is likely to vary over time and by what they are looking for, as well as how they prefer to look for it. In essence, however, they either directly access retailers' websites (perhaps having used a search engine to locate it); or they use a search intermediary to look for and compare product information and prices that sellers provide on their or third parties' online platforms. How effectively they search can have implications for their range of choice and potentially what they end up paying.

### Buying without searching

9.16. We found that six per cent of the internet shoppers we surveyed had used neither a search engine nor a price comparison site in the last 12 months and hence must have gone directly to a retailer's website. However, the number of people going straight to retailers' websites for many of their transactions was likely to be much higher, because we also found that one fifth (20 per cent) of internet shoppers usually buy from one or two sites that they already know (many of whom may go directly to these).

9.17. Those consumers that do not search when internet shopping generally go straight to retailers they already know or have used before. Trust is a key factor here. Shopping at well-known retailers is important to consumers because of the distance and anonymity of internet shopping which means that consumers must invest more trust in online retailers' handling of their data, delivery and returns. These factors are difficult for businesses to demonstrate and consumers to verify. In our consumer survey, we found that 54 per cent of internet shoppers

[234] SearchEngineWatch.Com.

[235] PWC/IAB (2006).

we surveyed stated that they only bought from online businesses that they had heard of and, of these, 56 per cent did so because they trusted the security of these sites (and 20 per cent because they trust their delivery). If consumer fears are potentially overstated to some degree (see Chapter 4), they may be restricting their choice and possibly paying more. Indeed, our consumer telephone survey found that nearly three quarters (72 per cent) were willing to pay more for a product on a site that they were familiar with rather than use an unfamiliar site. See Box 9.1 for further discussion.

### Box 9.1: The role of brands: Advertising and attracting custom online

Retailer branding allows firms to differentiate themselves from each other. Consumers have preferences for different aspects of quality and service and (branded) retailers can satisfy these demands by offering trusted products and service. Retailer brands may be particularly important online due to the distance selling aspects which are difficult to contract for, including delivery, product description, data security and the anonymity of retailers. A well known brand can indicate to consumers how trustworthy or how high quality the retailer is, and retailers spend substantial amounts developing their reputation.

Stakeholders raised these issues with us. The economic literature indicates that, whereas commentators had expected the internet to ‘commodify’ many products, reducing the role of retail brands, retailer brands remained important. Data on consumer behaviour on price comparison sites shows that those consumers who have indicated that they are sensitive to delivery are less sensitive to price and four times more likely to buy from a well known brand (Smith and Brynjolfsson (2001)).

Data on prices shows that unexplained differences in prices between retailers can, in part, be attributed to the willingness of consumers to pay a premium at branded retailers (Pan et al (2002)). For example, Baye et al’s (2002) US study of branding and price dispersion, using evidence from shopper.com, found that retailer branding accounted for 17 per cent of price dispersion. Another study using prices found that consumers are willing to pay a premium of 8.7 per cent for books and 8.6 per cent for CDs, for example, at a bricks and clicks retailer compared to internet only or pure play retailer (Smith and Brynjolfsson (2001)).

And these economic studies are supported by data in a separate UK survey by YouGov (2006) which found that the maximum consumers would spend online with a less well known store is a mean of £275 compared to £973 online at a well known brand/high street store website.

Well known brands are not always the most popular online, however, according to market research by Which? (2006), which found that consumer preferences were low for the online shops of some high street names due to consumer perceptions of poor service and/or range.

## The importance of searcing

9.18. Search sites play a significant role in choice of retailer and product. Our own research found that 47 per cent of internet shoppers had used a price comparison site and almost all (94 per cent) had at some point used a search engine to choose which website to buy from. Hitwise data also shows the importance of search engines, which accounted for 35 to 36 per cent of visits to retailers over October 2006 to February 2007.

9.19. Despite widespread use of search tools, however, empirical studies of consumer behaviour indicate that the depth of their use is limited. It appears that consumers do not always make the best choices, or search widely online. For instance, search intermediaries told us that most consumers do not search beyond the first few results presented at the top of the page. A number of economic and marketing studies confirm this, finding that when consumers search for items to buy hardly any view search results beyond the first page of results; most do not click through to more than one link; and on average a consumer spends 11 seconds reviewing search results (see Box 9.2).

### Box 9.2: Consumers' extent of search

**Number of links viewed:**

- Brynjolfsson et al (2004), found that only 16 per cent of consumers clicked through to more than one link and only nine per cent of consumers searched subsequent results pages.
- Similarly, Ellison and Ellison (2004), found that demand for a product is dependent on its position on the results list.
- Consumer Reports WebWatch (2003) found that 88 per cent of links chosen by consumers were within the first page.
- Johnson (2004), found that search is limited to 1.2 book sites 1.3 CD sites and 1.8 travel sites a month in the three categories.
- Jansen (2000) showed that 76 per cent of users did not go beyond their first query.

**Price:**

- Baye (2004) found that only 13 per cent of consumers on average purchased from the lowest price search result retailer. A firm listed first on a search results page, even when not ranked by price, still benefited from 17.5 per cent higher demand on average than when it was listed second. This is despite the ease with which the consumer can usually reorder the results by lowest price.

**Time:**

- De Vos and Jansen (2007) found that consumers spend only 11 seconds viewing search results when shopping.

9.20. Our own research also found limits to the extent consumers mix their use of search tools: 27 per cent of online shoppers stated that they have used only one price comparison site to search for things to buy, and 58 per cent used only one search engine.[236] Taken together this suggests a significant proportion of consumers could search more actively or effectively when internet shopping.

[236] These findings are from our online survey of relatively experienced internet shoppers, so may be biased towards wider search compared to less experienced internet shoppers.

9.21. There are a number of reasons why consumers might not search widely, including:

- **Information overload.** Chiang (2006)[237] studied how consumers search for items to buy online and found that the difficulty of processing all the information by consumers limited their search. Studies with similar arguments include Rowley (2000).[238] Participants in our focus groups confirmed that this could be a problem, citing a sense of being overwhelmed with information. Many claimed to only look at the top three or four results of a search:

  *'You put in the words and 300 sites come up and then I give up'* (Internet shopper, Cardiff, older).

- **Convenience.** Chapter 3 noted that convenience is the main draw for most internet shoppers, ahead of perceived lower prices. Some consumers will be willing to pay more for this convenience, and convenience may be a stronger factor than finding lower prices.

- **Underestimated search benefits.** Consumers will seek further prices if they expect that the likely savings are greater than the cost of the search in time or complexity.[239] Given the apparent ease of search, consumers might believe that the benefits of additional search are low. Indeed, we found that 57 per cent of those internet shoppers who only use one price comparison site or search engine stated as a reason that one search intermediary produces enough choice.

9.22. Where consumers are internet shopping for convenience reasons it may be rational not to search widely. But where consumers are underestimating the benefits of wider search they may miss out on good deals which they would have been willing to look for. Indeed, our research shows that it is important for consumers to search widely when internet shopping for the following reasons, which we consider in more detail below:

- **online price variations** can be substantial, so consumers might potentially save very large sums if they search widely

- **limitations to the information provided by search intermediaries**, such as whether they include advertising, as well as the traders and prices they list, can mean shoppers will gain by using more than one.

## Price variations online

9.23. Looking at prices for electrical and music items, our review of websites found that the most expensive prices for similar products were on average 30 to 60 per cent higher than the least expensive price.[240] Our review of prices only focused on these two sectors,[241] but empirical studies have found significant price variations online in other sectors (see Box 9.3).

[237] Chiang (2006) Pages 9-11.

[238] Rowley (2000).

[239] Diamond (1987).

[240] This figure ignores the most expensive and least expensive 10 per cent of prices of the electrical items. The most expensive price found for each electrical product using the entire range was 40-120 per cent dearer than the cheapest price found for each product.

[241] Our review of prices did not cover auction sites or travel because comparisons would be too difficult between items that might differ substantially.

9.24. These price differences were also apparent when comparing the results of search intermediaries. Our independent website review of eleven price comparison sites[242] found significant price dispersion between the lowest prices for the same item on different price comparison sites, due in part to the limited number of retailers listed on some (see para 9.33 below).

9.25. For instance, the lowest prices of the electrical items looked for on ten different price comparison sites varied on average (median) by 35 per cent. The review estimated that if a consumer visited only one of ten comparison sites they have a 50 per cent chance of finding one of the five lowest prices. If consumers are not aware of this they may miss better deals.

### Box 9.3: Empirical papers find that price dispersion online is significant[243]

Which? (2005) found significant price dispersion for a number of popular electrical products in the UK, as well as frequent changes in the cheapest internet retailer.[244]

Baye et al (2004) used daily prices for the 1000 most popular products on the US price comparison site 'shopper.com' in 2000 and 2001. They found that price dispersion was significant in product categories however many competitors there were, with an average range in prices from lowest to highest of 40 per cent. Using the same data Baye et al (2002) found that, of these 1000 most popular products, the lowest listed price in each category was 16 per cent below the average price.

Pan et al (2001) collected prices from a number of US price comparison sites in 2000 for a number of identical products within eight categories including books, CDs and consumer electronics. In these categories the highest average price difference, comparing lowest and highest price, was 51 per cent, for CDs, and the lowest 26 per cent, for laptops.

Prices can also vary significantly over small periods of time. Baye et al's (2003) paper found, using US evidence from shopper.com, that retailers changed prices regularly online. The lowest prices, as well as the retailer offering the lowest price, varied substantially. This indicates that it is profitable for retailers to apply short-term price promotions in order to keep their prices unpredictable and hence partly avoid price competition. It also means that shoppers need to check regularly for price changes.

[242] In this section, we sometimes refer to reviewing ten and sometimes 11 price comparison sites. This is because we looked at nine sites that provided prices for both music and electrical items, and one site that provided prices for electrical items only, and another that provided music prices only. Altogether, therefore, we looked at 11 price comparison sites, but when referring to results solely for electrical items or for music items, the number of comparator sites being compared was ten.

[243] Annexe F, chapter 5 lists the economic papers that have found some or significant price dispersion online.

[244] Which (2005).

## Search intermediaries – limitations to the information they provide

9.26. Search intermediaries need to make their sites attractive both to consumers and to advertising retailers, which may create some tensions. However, if consumers do not realise that some links are listed more prominently because the business has paid for it, and if they tend not to search widely, then they may not necessarily find the best offer.

9.27. Research has found that advertising on search intermediaries is often poorly disclosed, particularly on price comparison sites.[245] Although this research considered American sites, the same business model exists in the UK. Our independent review of 11 UK price comparison sites found that the disclosure of advertising and paid for inclusion was not always clear and easy to find. Of the 11 sites, only:

- Four had easy to find disclosure of paid for inclusion
- Four confirmed paid for advertising
- One confirmed paid for prominence

9.28. The evidence on whether consumers know that retailers can pay to be in search results is mixed. Our survey found awareness to be surprisingly high: 61 per cent of internet users claimed to be aware that comparison sites 'compare prices for a limited number of retailers that pay to be included', and 50 per cent were aware that they may 'place a retailer higher in the results list if the retailer pays'. The findings were similar for search engines, and awareness did not vary by experience.

9.29. However, participants in our focus groups revealed some uncertainty about price comparison sites, with participants who used the internet relatively infrequently for shopping not always being able to identify a price comparison site from other sites online. Indeed, most other evidence suggests that consumers have limited awareness of advertising on search intermediaries. For instance, Ofcom recently found that only 25 per cent of adults know how search websites are funded and 51 per cent do not.[246]

9.30. Whatever the true level of awareness, however, it seems clear from the evidence described earlier that consumer search online is not always effective or deep. This is important, because consumers cannot be guaranteed to find a good price using just one search site.

9.31. Price comparison sites can provide a very valuable range of information to consumers, and typically enable them to sort by key variables. For instance, six of the 11 price comparison sites we looked at gave consumers the choice of how results were listed before commencing their search. Furthermore, in well over half the searches undertaken (62 per cent) for electrical goods, the lowest price was the first e-tailer listed on the default search setting.

9.32. However, our review also found some limitations to the information some sites offer. For instance:

- Price data were not always up to date. In 30 per cent of cases the price was higher on retailer site linked to than stated on the comparison site. Despite this only two of the 11 sites studied indicated how often prices were updated.
- Of the 11 price comparison sites only one scored a 100 per cent success rate giving the correct final price for all successful searches made.

[245] Consumer Reports WebWatch (2002, 2003, 2004 and 2005), and Federal Trade Commission (2002).

[246] OFCOM (2006). In the US, Consumer WebWatch's (2003) ethnographic study found that few consumers recognised sponsored links and that nearly half the links consumers selected when searching for an item to buy. Hotchkiss, Garrison, and Jensen conducted a survey study with 425 respondents. The researchers report there is confusion concerning sponsored links, with more than 30 per cent of the participants unable to identify properly the sponsored links on a search engine. The Pew Internet and American Life Project (2005) survey of 2,200 Americans found that only 38 per cent of searchers reported awareness of the distinction between sponsored results and non-sponsored links. Less than 17 per cent stated that they can always tell which results were which. Greenspan (2004) found that the higher the position of a sponsored link the more likely it was to be clicked.

9.33. Furthermore, when the reviewers searched for 20 electrical and hard copy music items they found that the number of online retailers offering each product in question varied substantially on each price comparison site. For many products, the number of retailers offered by different price comparison sites varied from one to 12. The largest variation was for a classical CD album, where one price comparison site offered only one retailer, but another offered 42. In many cases price comparison sites listed only a single retailer that offered the specific item.

9.34. Our independent website research also found that only five of the eleven price comparison sites looked at provided explanations of which online retailers they covered. Of the other six, two were thought by the investigators to have given the impression that they searched the whole UK web.

9.35. Consumers might limit their search if they are unaware of these variations and limitations. To ensure that they find the best deals, therefore, consumers should search widely and use more than one search site. Using the findings of our survey, we estimate that up to one million internet shoppers restricted their search to only one site because they did not know the limitations of search intermediaries.[247] Assuming that these consumers would find the kind of lower prices identified in our review of websites if they searched more extensively,[248] they could be **missing potential savings of £150 million to £240 million per annum**, as they wrongly assume that they may have searched sufficiently. This excludes those shoppers who do not search more widely due to convenience reasons, besides their unawareness about the limitations of search intermediaries.

## The clarity of information

### Clarity of pricing

9.36. However, even if consumers are aware of the value of wide and deep search online, they may be hindered by a lack of clarity in the information presented to them – especially price information. Our independent review of websites looked at prices for 11 music and 12 electrical items across 150 retailing websites (100 retailers for electrical items and 50 retailers of music products). It found some substantial differences in the initial and final prices on some websites, as well as some problems with the clarity of the information on products. For instance:

- in most of the cases it was not immediately clear whether the first price displayed included delivery (77 per cent for electrical items and 85 per cent for music CDs)
- in a high proportion of electrical cases (62 per cent), the final price was higher from the price initially stated. This was also the case in 38 per cent of searches for all music products under investigation. The increase was almost always delivery costs.[249] Table 9.1 gives some examples of the price increases observed in our website review for electrical and music products

[247] Stating either that (a) all search engines produce the same choices or (b) all price comparison sites produce the same choice or (c) price comparison sites' results are not biased by restricting their search to a limited number of retailers. This excludes those internet shoppers who limit their search because of convenience reasons.

[248] As the website review found that if a consumer visits only one out of ten comparison sites they only have a 50 per cent chance of finding the fifth lowest price and given the sometimes very limited number of listed online retailers and high price variation online, this is a reasonable assumption.

[249] These are provisional estimates by OFT analysts using data from the FDS website review. Of 254 searches for hard copy music, 38 per cent indicated an increase in price from the initial price displayed to the final 'checkout' price. This increase was on average (median) 16 per cent higher. Of 434 checks on electrical items, 62 per cent indicated a median price increase of eight per cent. There were three music and four electrical checks where the price decreased, however, including or excluding this small number of cases (all of which were small in value) has no effect on the value of the average increase.

- when searching for hardcopy music, researchers were unable to find details on delivery on any pages seen before entering payment details on around one in ten (11 per cent) of the websites.

**Table 9.1: Some illustrative examples of price increases for electrical and music goods[250]**

| Item | 'First price' (lowest – highest) | 'Checkout price' (lowest – highest) | Average (median) additional charges |
|---|---:|---:|---:|
| Micro Sound System | £48.99 – £149 | £49.99 – £149 | 10% |
| Hard Copy CD Album | £6.47 – £14.99 | £6.97 – £18.30 | 17% |
| Dishwasher | £215.23 – £339 | £219.99 – £372 | 8% |

9.37. Our independent review also looked at 100 sites selling flights, examining 167 flights. This found that:

- in 47 per cent of cases the checkout price was higher than the original price[251]
- in over a third (37 per cent) of flight searches, airport or other taxes were either not included in the initial price or it was unclear to the potential customer.

**Table 9.2: Summary of price increases in the three sectors**

| Sector | Proportion of websites adding charges | Median of additional charges[252] |
|---|---:|---:|
| Electricals | 62% | 8% |
| Music | 38% | 16% |
| Flights | 47% | 19% |

9.38. Of these additional charges, online shoppers in our online survey said that the type most commonly experienced were delivery charges (experienced on some occasion by 49 per cent of consumers), followed by booking fees (33 per cent), credit card charges (30 per cent), and tax (22 per cent).

9.39. In over half of cases (54 per cent), the additional charge had been made at the point of confirming the purchase, and in 25 per cent of cases at the point of selecting the payment method. In two per cent of cases, the charge had been added on delivery, and in one per cent had the charge been added on receipt of the bill or statement.

9.40. Taking one of our example case study sectors, we looked in more detail at the prices for flights and found some substantial price differences, as well as a variety of different types of additional charges that might be added later in the buying process (see Box 9.4). Having to check multiple, and often variable, additional charges could make the search process more difficult for consumers.

[250] Source: OFT analysis of data from the Website Review (Annexe L). The price ranges shown in the table relate to the lowest and highest prices found for each product at the initial and checkout stage, respectively.

[251] For eight per cent of the 167 flights checked, final check out prices were lower than the initial price. These average a median decrease of just four per cent and are mainly due to online offers.

[252] The median is used, to avoid the results being skewed towards any outliers.

### Box 9.4: Case study example – clarity of pricing when buying air travel online

In 2005, online air transport sales to households totalled £2.7 billion (13 per cent of all internet sales to UK households), having increased by 42 per cent on the previous year.[253]

Airline tickets often have extra charges added to the advertised price at a later stage in the purchasing process. These charges can be fixed or flexible, and compulsory or optional. Examples include airport tax, fuel surcharges, baggage fees and credit card fees. We found that for 47 per cent of the individual flights we sampled, the final 'check-out' price was higher than the initial price.[254] Where prices changed, the median increase between first and final price was 19 per cent. However there were some much larger increases: for instance two tickets from Bristol to Malta originally advertised at £116 increased by 211 per cent to £310, once all charges were added.

Although a median increase of 19 per cent is only slightly higher than the other two sectors we looked at, the price ranges were much bigger. In 41 cases, the price of a flight had increased by 30 per cent or more once additional charges were added. Taking into account all the changes (including some large outliers), the mean increase for the flight sector was 131 per cent, compared to 20 per cent in the music sector and 10 per cent in electrical sector.

Furthermore, our review found that while delivery was the only substantial additional cost in the music and electrical sectors, there were several different types of charges that might be added to the cost of a flight. Some of these charges are fixed and non-optional for all passengers (for example air passenger duty (APD), airport tax, fuel supplements), and some are not (for example transaction/credit card charges, airline failure cover, charges for pre-bookable seats and in-flight meals).

These findings highlight how important it is, but also how hard it can be, for consumers to make like-for like comparisons. However, there are developments which may have important implications for the clarity of future ticket prices:

- In February 2007, the OFT warned travel providers to include all fixed non-optional costs in their basic advertised prices. In May, having reviewed advertising, it announced its intention to bring enforcement proceedings against those airlines still failing to comply (see Box 9.5 below).[255]
- The EC is considering a proposal for a revision of the Third Package for air transport, which is likely to include an obligation to quote all flight prices inclusive of non-optional taxes, fees and charges.[256]

[253] Source: ONS analysis of the 2005 e-commerce Survey of Business. Note: these data represent the sales of businesses with 10 or more employees. 'Air transport' is defined by the two digit SIC '62' and is not considered the optimum for sectoral publication.

[254] We did not test how prices varied by different types of provider, although individual airlines may vary in the nature of the services they provide and their pricing strategies, and consumers may take this into account when comparing prices and making their choice.

[255] See the OFT press release at: www.oft.gov.uk/news/press/2007/72-07.

[256] This is the third package of EC measures to liberalise aviation. See: ec.europa.eu/transport/air_portal/consultation/doc/2003_05_15/consultation_3_package_en.pdf.

### Clarity of pricing: Regulatory protections

9.41. As we have seen in Chapter 6, in addition to the information requirements imposed by the DSRs and ECRs, many other pieces of legislation protect consumers against misleading pricing. Two of particular relevance are outlined in Box 9.5. Briefly shoppers buying through any retail channel, including websites, can expect traders:

- To tell them the full price they will have to pay (including delivery and other charges) before they commit to buying
- Not to make false or misleading statements, or create misleading impressions

### Box 9.5: Price clarity: Regulatory protections[257]

#### Consumer Protection Act 1987 ('CPA')

Part III of the CPA prohibits misleading price indications Section 20 of the CPA makes it a criminal offence for a person in the course of business to give consumers an indication (by any means) which is misleading as to the price of any goods, services, accommodation or facilities. Enforcement of CPA is the responsibility of Local Authority Trading Standards Services.

The Code of Practice for Traders on Price Indications 1988 (the Price Indications Code)[258] gives practical guidance on the requirements of section 20, and applies to price indications given by email or on a website.[259] Compliance with the Code is not mandatory, but it will be taken into account when considering whether an offence under section 20 of the CPA has been committed.

The Price Indications Code indicates that traders should make clear the full price consumers will have to pay for a product, so that consumers are always aware of the total cost including, for example, postage, packing, delivery charges, insurance etc. before they commit themselves to the purchase.[260]

Considering the example of flight prices described in Box 9.4 above, under the CPA, businesses which advertise holiday or travel prices on a website should include any non-optional extra charges which are fixed amounts as part of the basic price, and not as additions (unless they are only payable by some consumers in which case the business should specify, near to the details of the basic price, either what the amounts are and the circumstances in which they are payable, or where in the brochure etc. the information is given). Details of non-optional extra charges which may vary (or details of where in the brochure etc. the information is given) should be made clear to consumers near to the basic price.

[257] In 2008, Part III of the CPA will cease to have effect and the CMARs will also be revoked when the Consumer Protection from Unfair Trading Regulations are brought into force.

[258] DTI (2005a).

[259] Paragraph 2.1.1.

[260] Paragraph 2.2.1.

### Control of misleading advertisements regulations 1988 ('CMARS')

CMARs provide protection against misleading advertisements.[261] An advertisement is misleading if in any way, including its presentation, it deceives or is likely to deceive people and is therefore likely to affect their economic behaviour or injure a competitor of the advertiser. An advertisement can be misleading if, for example, it contains a false statement of fact, promises to do something with no intention of carrying it out or creates a false impression (for instance by leaving out important facts) even if everything stated in the advertisement may be literally true.

Before considering complaints under CMARs, the OFT will normally need to be satisfied that the issues should not be resolved by using 'established means' such as by referral to the Advertising Standards Authority (see below) or the appropriate Trading Standards Service.[262] The OFT may seek a court order to prevent the publication of misleading advertisements.[263]

## Clarity of non-price information

9.42. Consumers may not only be confused or even misled by unclear pricing – their ability to compare and choose can be undermined by other unclear information. Poor information may include omitting important details on for instance, restrictions on usage or whether an item is out of stock. Some commentators[264] have also suggested that retailers may deliberately attract consumers with low prices for products whose poor quality is masked, in the hope that consumers cannot be bothered to search elsewhere and buy a more expensive product.

9.43. Taking music sales for instance, we found that it might not always be clear to consumers what they were getting. Some said that they had unexpectedly experienced restrictions on how they could use the songs they had bought (Box 9.6).

### Box 9.6: Case study example – clarity of information when buying music downloads

With the growth of file sharing of copyrighted music in recent years, the major music labels[265] have commonly required Digital Rights Management (DRM) software to be applied to their catalogues before they will allow music to be purchased.

DRM places technical limitations on what a purchaser of a track can do with it once they have it. DRM can be used to cap the number of playback devices, computers or CDs to which the track can be transferred. It can also limit the tracks to a specific model of playback device. These limitations may also depend on how consumers buy their music – by purchase or subscription:

- **Subscription model:** under some subscription services, a subscriber pays a monthly fee to access a catalogue of songs, which they can only play so long as they subscribe. In this case DRM has created a new business model for selling music online.

[261] Advertisements are defined as 'any form of representation which is made in connection with a trade, business, craft or profession in order to promote the supply or transfer of goods or services… rights or obligations' (Regulation 2(1)). Responsibility for enforcing CMARs is split between broadcast and non-broadcast advertising. Radio and television advertisements are the sole responsibility of the Office of Communications (Ofcom).

[262] See: www.tradingstandards.gov.uk. The Code which came into force on 4 March 2003 supplements the law and fills gaps where the law does not reach. OFT does not have any powers under CMARs to clear advertising copy in advance of publication but businesses may be able to get advice from the Committee of Advertising Practice ('CAP') an industry body that created revises and enforces the British Code of Advertising Sales Promotion and Direct Marketing (www.cap.org.uk).

[263] Section 211 EA02.

[264] Ellison and Ellison (2004).

[265] Sony BMG, Warner, Universal and EMI.

- **Purchase model:** where the service charges a one off fee to buy and download a track. In this case DRM limits what consumers can do with the music after purchase.

In this study, we did not consider the issue of whether DRM should be applied to music. However, studies have found a significant lack of awareness and understanding of DRM amongst the public. In 2005, the European Commission[266] found that 62 per cent of UK consumers had never heard of DRM and only 4 per cent had a clear idea of what it was. Additionally 77 per cent of users did not know if their usage would be limited. This broadly corresponds with our own online survey which found that 44 per cent of respondents had been unexpectedly restricted after they had bought music via download.

The recent Gowers Review of Intellectual Property[267] suggested that the DTI investigate developing a labelling convention. A similar recommendation was made in June 2006 by the Parliamentary All Party Internet Group (APIG).[268] Similarly the European Commission recently released a report[269] recommending that the revised Copyright Directive should disclose 'the scope and characteristics of the DRM' to inform consumers. The OFT supports measures to improve consumer understanding of DRM and any limits it places on their use of music. Clearer labelling on physical products and on websites selling music could help consumers to make more informed decisions. In Germany download services are legally required to notify consumers of any DRM they employ and the restrictions on them after sale.[270]

9.44. Looking at another of our case study sectors, flight sales, the rise of the internet itself may have been a factor in a potential lack of clarity in whether consumers have financial protection against their flight operator going bust (see Box 9.7).

### Box 9.7: Case study example – financial protection information when buying air travel online

The entire market for air travel has been transformed by the internet, with the appearance of internet-based 'no-frills' airlines.

The Package Travel Directive (PTD)[271] requires companies selling packages to meet specified consumer protection requirements. In the UK the PTD is implemented by the Package Travel Regulations (PTRs).[272] The financial protection provisions (i.e. the refunding and, if necessary, repatriation of consumers if their travel company goes bust) where the package includes a flight is part of the ATOL (Air Travel Organisers' Licence) scheme.

[266] INDICARE (2006).

[267] Gowers (2006).

[268] APIG (2006).

[269] University of Amsterdam (2007), See Page 133.

[270] Article 95a, German Copyright Act.

[271] Council Directive 90/314/EEC on package travel, package holidays, and package tours (OJ No L158, 13.6.1990).

[272] The Package Travel, Package Holidays and Package Tours Regulations 1992 (SI 1992/3288). These were amended in 1998 (SI 1998/1208).

If a consumer purchases a scheduled flight direct from an airline (or an agent of the airline), there is no automatic financial protection under ATOL, unless it forms part of a package. The internet has made such purchases easy, and they are now becoming more common.

The existing regime arose in the pre-internet era and complexity in the law, combined with the rise of web-based sales, means it is now not always clear what protections apply to which products or providers. This situation is compounded by poor consumer awareness of the available protections and as a result, growing numbers may be unprotected.[273] In particular, there has been some confusion as to whether the definition of a package covers the format common in online travel purchasing, where consumers can choose the individual elements of a holiday, such as travel and accommodation from a selection.

We found that consumers buying from sites selling flights could be offered accommodation in various ways, including by linking to another area of the same site; linking to another provider (sometimes with branding similar to that of the originating site); travel agents selling traditional type package holidays; and others providing more flexible services. It was often difficult to identify with whom the consumer would be forming a contract and whether what was being sold was a 'package' or not. Information on what financial protection, if any, applied was not presented in a consistent format or sometimes not presented at all.

In this study, we did not consider the issue of what financial protections should be available to consumers buying flights online. There are, in any case, ongoing developments in this area.[274] For instance, at the time of writing, the DTI was due to consult on revised guidance on the coverage of the PTRs which aims to reflect a recent Court of Appeal decision[275] on the definition of a 'package' contained in the regulations, and which is also the definition in the ATOL regulations.

We support moves to bring clarity in this area. Consumers would benefit from being told if they are not covered by the PTRs and ATOL, so that they can consider whether they want to take out additional insurance. They should also look to see whether any travel insurance policy automatically offered when they make a travel purchase includes insolvency protection if not otherwise protected and, if it does not, consider whether to switch to one which does.

[273] A 2005 CAA survey found that 36 per cent of respondents believed that ATOL would protect them if they booked directly with a scheduled airline, but 54 per cent did not know. And 22 per cent thought ATOL would protect them if they booked directly with a 'low-cost' airline, but 59 per cent did not know. Our own survey asked consumers who had bought a flight online direct from an airline whether it was made clear that their money was not automatically protected if the airline ceased to trade: 65 per cent said this was not clear, and 26 per cent said they did not know, or did not check. Research by the Civil Aviation Authority (CAA) shows that the proportion of leisure air passengers who were ATOL protected decreased from 98 to 66 per cent between 1997 and 2004 (CAA (2005)).

[274] Most airlines have so far, through voluntary agreements, agreed to honour each other's tickets in the event of collapse, although this may not apply to some no-frills carriers. There is also growth in the inclusion of insolvency protection in travel insurance policies. At the EC level, the PTD is being reviewed as part of the review of the consumer protection Directives (consumer acquis). In the UK, DfT has been working with the industry on voluntary measures for repatriation and to sell scheduled airline failure insurance.

[275] In October 2006, the Court of Appeal dismissed an appeal by the CAA against a court decision that a Guidance Note on the applicability of the PTRs and ATOL Regulations, published by the CAA, was unlawful. The judgement highlighted the difficulties in defining exactly what is a 'package' for the purposes of these regulations.

9.45. Self regulation could also play a role in addressing misleading online advertising (see Box 9.8 on the role of the Advertising Standards Authority). At present, the CAP Code covers commercial emails, sales promotions, and advertisements in paid-for space, such as banner advertisements.[276] However, the Code does not apply to website content.

### Box 9.8: The Advertising Standards Authority ASA

The ASA is a self regulatory body, independent of both government and the marketing industry. It is responsible for dealing with complaints about adverts in non-broadcast media under the British Code of Advertising, Sales Promotion and Direct Marketing (the 'CAP Code'). Amongst other things, the rules of the Code require that advertisements do not mislead consumers, and that advertisers hold evidence to prove the claims they make about their products or services before an ad appears. Also advertisements are not allowed to cause serious or widespread offence.

While some complaints can be resolved quickly, others may need formal investigation. If so, the ASA Council will rule on the matter and publish their adjudication. Once the Council has made a decision, the advertisers must make sure that the ruling has been followed, whether that means changing an ad or withdrawing it. If a complaint is upheld, the advertiser is not allowed to use the ad or the advertising approach in any future marketing communications. The ASA[277] lists a number of potential consequences for advertisers:

- The ruling will be published on their website, often leading to bad publicity for the advertiser
- Media owners and broadcasters will refuse to run ads that break the Codes
- Direct marketing companies can have benefits such as Royal Mail bulk mailing discounts removed if they persistently flout the Codes
- The advertiser can be referred to the Office of Fair Trading for misleading ads and impermissible comparisons and broadcasters can be referred to Ofcom for persistently airing ads that break the rules.

9.46. The ASA's latest Annual Review noted a rise of 33 per cent on the previous year of complaints about the internet. It stated: *'the internet is now the second most complained about advertising format – a rise unmatched in any other media. Yet the boundaries of regulatory responsibility online are still unclear.'*[278]

9.47. Given the growing importance of online advertising and the apparent increase in complaints about the internet content covered by the CAP code, we would welcome the Committee of Advertising Practice considering extending its remit to cover websites as well. As a form of self-regulation, this could help to bolster and complement the regulatory protection provided by the Consumer Protection from Unfair Trading Regulations (CPRs) in the future. It could also help to increase consumer trust in the quality of the information presented to them, as well as underlining for businesses the importance of clarity when advertising online.

[276] 1.2 q of the Code.

[277] www.asa.org.uk.

[278] ASA (2006).

## The importance of providing clear information

9.48. Just as on the high street, online retailers need to advertise to grab attention, and this process can help match consumers to products. However, businesses should not mislead consumers for example by applying false or misleading descriptions, or by advertising prices that do not correspond to the actual prices charged.

9.49. Poor information provision by retailers can undermine competition and affect consumer behaviour. It makes it hard for consumers to compare final prices when searching online, and complicates their decision-making by requiring them to click through to additional pages or even register with a site to find the final price. In other words, it increases their 'search costs'. It can also lead them to buy products with conditions and restrictions on them that they were unaware of. In the worst instances, consumers may actually find that they have paid more than they thought they had.

9.50. Our research also detected considerable consumer annoyance: almost all respondents (91 per cent) stated that they thought that only the final price should be advertised. We also found that over three quarters of people (77 per cent) thought that unexpected additional charges were more of a problem on the internet than on the high street.

9.51. In economic literature, it has been argued[279] that the provision of unclear information to consumers is more likely online. Internet pages can almost costlessly offer a variety of add-ons and prices, including the low price that will attract consumers in the first place. These add-ons can be mentioned on pages later in the process when consumers may well resort to paying them rather than start the search process again. Internet retailers may also be able to change prices and offers more rapidly by compiling information in real time.

9.52. A number of economic papers have also discussed the incentive of online retailers to be unclear in their pricing, in the face of the potential of the internet to increase competition. One empirical study[280] found that this can be a profitable strategy for online retailers because a sufficient proportion of consumers go on to purchase the original item despite unexpected charges or lower quality than expected. This is because the search costs, including the time entering data and registering with a retailer, involved in internet shopping while arguably relatively low are not trivial.

9.53. Although we found that additional charges are common and annoy consumers, we also found that 77 per cent of customers who had experienced them went on to buy the item anyway. Of those that went on to buy, 36 per cent said they still could not buy it elsewhere any cheaper while 27 per cent bought anyway because the 'price increase was not that large'.

9.54. Ultimately, 13 per cent of those that went on to buy despite the charges, did so because they did not want to search again, enter their details again or had no choice because the purchase had been processed. These are the consumers that were drawn in by the low initial price and then resorted to buying the item to avoid the effort and time involved in searching again. This is still a lot of people: on the basis of our survey results we estimate it could amount to as many as 1.2 million internet shoppers who might have changed their search behaviour had they expected the charges.

[279] Ellison and Ellison (2004).

[280] Ellison and Ellison (2004) assessed data from a price comparison site and concluded that it is straightforward for retailers to advertise apparent loss leaders. Once the consumer has realised that the good is not as attractive as on first sight, enough consumers do not search again to make the behaviour sustainable for the retailer.

9.55. Taking our findings of unexpected charges in our case study sectors, we found that these add up to approximately £14 million in the flights sector, £6 million in the electrical and £3 million in the music sector (all per annum). These figures suggest that, if extended to all internet shopping sales, consumers who were unaware of the additional charges prior to the purchasing process could pay £60 million to £100 million each year in unexpected charges, or approximately £50 to £85 per unaware online shopper.[281]

## Conclusions

9.56. Provided they are used well, tools such as search engines and price comparison sites can help consumers to make informed choices and save money. However, we found that some consumers could benefit from searching more effectively online, particularly given limits to the numbers and range of traders listed by price comparison sites.

9.57. We also found in many cases, the final price was very different from that first shown. Lack of clarity in pricing and other information can undermine consumer choice. This is an issue that the OFT takes seriously: we recently announced our intention to bring enforcement action against a minority of airlines that had failed to comply with our warning to include all fixed non-optional costs in their basic advertised prices.[282] We will continue to take action in this and other sectors where there is clear evidence of detriment to consumers. There could also be scope to improve the quality of information provided to consumers by extending advertising self-regulation to websites.

### Next steps

9.58. It is important that consumers appreciate the limitations of search sites and use them as effectively as possible. We will develop ways to raise awareness of how shoppers can make best use of the tools available to them. We will also explore with the Committee of Advertising Practice whether their remit could be extended to cover websites. Our work on raising awareness will include making clear to businesses their obligations when presenting information to consumers.

[281] Not all of this is consumer detriment, because some of these charges may still have to be paid. However, even if the shopper searches widely, if they are not presented with the full costs upfront then their decision may be more difficult and time consuming.

[282] See OFT Press Release at: www.oft.gov.uk/news/press/2007/72-07. Separately, the Association of British Travel Agents (ABTA) has issued a reminder to its members that its Code of Conduct requires them to include all fixed non-optional costs, such as taxes, in the basic advertised prices of their holidays. ABTA has said it will rigorously enforce this Code against travel companies who do not comply.

# 10 'ONLINE AUCTIONS'

## Summary

The internet has enabled the creation of 'online auctions' – vast electronic market places, bringing together buyers and sellers of an enormous range of products. These are a valuable development, with millions of successful transactions every year. A recent estimate was that purchases from online auctions using payment cards in 2005 accounted for 79 million transactions and spend of £2.8 billion. Over one-tenth of the time people are online is spent visiting online auction sites.

Their advent has also greatly facilitated the trade for certain products, such as niche and second hand items, enabling people to sell unwanted items easily and businesses to use the market place as a virtual shop front.

While the bulk of transactions are completed successfully on online auctions, we found that many non-users and users we surveyed still had some concerns about using them. Also a relatively high proportion of users surveyed had experienced problems – typically related to delivery, contact with the seller and perceived scams. Although the value of the items was typically modest and a high proportion did not complain, of those that did nearly four in ten (39 per cent) had given up trying to achieve a successful outcome.

Generally, users of online auctions are protected in the same way as other online purchasers. There is some uncertainty as to whether the DSRs apply, although the ongoing EC Review may help to resolve this.

What rights consumers have depend on from whom they are buying. We found that 60 per cent of consumers wanted to know whether they were buying from a business. It may, however, be difficult even for sellers to tell at what point they are trading in the course of business. The failure of some businesses selling through online auctions to provide their name and address to buyers can also be a problem.

Where things go wrong, the legal liability and legal responsibility for consumer redress typically rests not with the auction platform but with the seller in question. Given this, consumers need to be aware of the risks involved in buying on such sites and to take sensible precautions.

## Next steps

We want to work with the online auction sites and others to ensure that sellers on such platforms know how to comply with their legal obligations to consumers. Our strategy to improve consumer and business awareness will include advice in this area as well as how to deal with deceptive practices.

We will encourage sellers to self-assess to ensure they are meeting their obligations. We want to investigate further how businesses selling via online auctions can be more clearly identifiable to buyers. Where businesses are not complying with regulatory requirements, and there is clear evidence of consumer detriment, we will take appropriate action to ensure that this is addressed.

We also want to investigate how the online auction sites are addressing issues like counterfeiting and sellers bidding up their items.

## Introduction

10.1. The internet has enabled the creation of large electronic marketplaces, which bring together buyers and sellers of a huge range of products. The most significant marketplaces are built around a competitive bidding process, and for this reason they are known as 'online auctions'.[283]

10.2. Many issues common to distance selling apply equally to online auctions. However, these marketplaces also raise specific issues for their operators and users, as well as for regulatory and enforcement agencies. In this chapter, we explore consumers' and businesses' use of online auctions and their experiences; as well as the problems that some may encounter and what legislation applies.

## Background

10.3. 'Online auctions' are generally marketplaces that provide services to facilitate trade by means of competitive bidding, although many also offer a platform for immediate sales. Examples include eBay and eBid. These sites are not like traditional auction houses. For example, they do not act as agent for the seller, nor prepare catalogue descriptions. Nor do they take possession of the items for sale on the site (see Box 10.1).

### Box 10.1: Online auctions and traditional auctions: When is an auction not an auction?

The term 'online auction' in this study is used to refer to the eBay or eBid form of business model, and not to traditional auction houses which may operate on the internet as an extension of their offline practice.

There is no statutory definition of an auction. It is generally held to be a manner of selling property by bids, usually to the highest bidder, by public competition. Auctions have a number of characteristics:

- a unique item or collection of items for sale
- each bid is an offer to buy
- the auction ends in a pre-arranged manner, such as on the fall of a hammer or the expiry of a deadline
- the winning bidder is bound by contract to pay for the items.

The clearest difference between traditional auctions and internet auctions is the absence of an auctioneer. In a traditional auction, the auctioneer acts as the agent of the seller, and uses their skills to obtain the highest price for the goods. The auctioneer will also normally take possession of the goods and be responsible for producing a catalogue for the sale, in which the goods are described.

[283] Although there are different types of 'third party platform' which enable sellers to sell products through them, we focused on those that include a competitive bidding process as one way of selling, because of the growing use of these sites and specific issues they raise. We also restricted our consideration to issues raised by the nature of these online marketplaces, rather than any specific issues that might be raised by the sale of particular types of products on them.

In online auctions, although the site operator does offer some services to the seller (and the buyer – see box below), it does not perform these traditional functions. This has led some authors to conclude that internet auctions are not 'auctions' at all,[284] although other commentators are of the view that it is 'strongly arguable' that such sites are acting as auctioneers, albeit to a limited extent.[285] An alternative argument is that since individual sales have the characteristics outlined above, they are each individual auctions – where the seller is acting as their own auctioneer.

10.4. 'Online auction' models can differ, but typically, sellers need to register as members to list goods for sale. Usually, anyone can browse, but generally they need to register before they can bid or buy. Members often register and trade under pseudonyms, although retailers using the sites as a platform often do not trade anonymously.

10.5. Membership of the sites can vary widely from individuals selling one-off items second hand, to established businesses selling new products and surplus stock in large volumes. It is also possible that 'hobby' sellers, through the process of systematically selling goods to make a profit, may become traders for tax purposes without fully understanding that they are in business.[286]

10.6. In addition to listing items for sale by competitive bidding, online auctions may enable sellers to list items for sale at a fixed price. Again, the site facilitates these transactions, but is not involved directly in them. Fixed price sales are increasingly important – in 2005, they accounted for 38 per cent of sales at eBay, with a rising trend.[287]

## How 'online auctions' work

10.7. The sites provide a number of facilities to buyers and sellers. These typically include the ability for members to communicate with one another, review feedback from other users, and to turn to dispute resolution services if they experience problems (see Box 10.2). In return they will charge sellers (but normally not buyers) a fee.

### Box 10.2: Facilities often provided to buyers and sellers by online auction sites

- The ability to **list goods for sale** on the marketplace. This may be as one off listings for consumers or as virtual 'shop fronts' for traders which allow the listing of many goods for sale in a shop format
- The ability to **search for goods for sale** on the marketplace
- **Communication** – The sites usually facilitate the exchange of messages between members so, for example, potential buyers and sellers can discuss the items for sale
- **Reputation mechanisms** – Auction sites rely on users trusting one another. They typically offer reputation mechanisms so that buyers and sellers can rate and comment on the experience of dealing with their counterparts

[284] For example, Riefa (2005) pp.34-36.

[285] Harvey and Meisel (2006), p.17.

[286] HMRC have produced guidance which considers potential tax liability for online selling on such sites. See www.hmrc.gov.uk/guidance/selling/income.htm (February 2007).

[287] Mintel (2007).

- **Advice/Guidance** – Most sites have guides on how to buy and sell on their marketplace, and often advice on safe trading
- **E-payments** – Sites may offer integrated electronic payments, sometimes via third parties
- **Dispute Resolution** – The site may provide a mechanism to help resolve disputes between members.
- **Protection for buyers** – The site may provide buyer protection to reimburse consumers under certain circumstances.

10.8. For sellers there are often two main fees – a listing fee and a final value fee. The listing fee typically depends on the reserve price and the item being listed, while the final value fee is usually a proportion of the sale price. However, business models vary in this fast moving sector. For example, some sites offer no listing fee and only charge sellers a proportion of the sale price. Sites also often provide special offers including no, or reduced, listing fees or completely free sale transactions.

10.9. The seller is responsible for describing the goods to be sold, making any stipulations as to payment and delivery and also sets the reserve price (if any) and the duration of the auction.

10.10. Buyers are generally not charged to use the platform. They are, in economics terms, the relatively scarce side of the market. They are not charged fees to use the platform because otherwise they might not use the market at all, reducing its value to all users. Sites and their users can benefit from a virtuous cycle of growth. Sellers benefit as more buyers join the site, and demand increases and becomes more varied. Buyers benefit as more sellers join, and supply increases and becomes more varied.[288] Some charges might be levied on buyers for related services such as e-payments.

## The growing importance of 'online auction' sites

10.11. A recent estimate was that purchases from online auctions using payment cards in 2005 accounted for 79 million transactions and spend of £2.8 billion.[289] Internet analysts Hitwise placed online auctions at the head of the online retail sector, accounting for the largest number of unique visits (20.9 million unique visits in December 2006).[290]

10.12. A number of online auction sites exist in the UK, including eBay and smaller rivals like eBid, CQout and QXL. eBay told us that their site had over 15 million registered users in the UK as of May 2006 (although some may be multiple accounts), and over 233 million worldwide as of Q1 2007. In fact, eBay.co.uk is one of the most visited websites in the UK,[291] with visits to their site accounting for 11 per cent of the total time spent on the internet in the UK.[292]

[288] An online auction can be characterised as a 'two-sided market' (also known as a 'two-sided platform', or '2SP'). See Armstrong and Wright (2005), Evans (2002), Evans (2005), Roson (2005), Evans and Schmalensee (2005), Dewan and Hsu (2001), Damiano and Li (2003), Belleflamme and Toulemonde (2004 and 2006), Ellison, Fudenberg and Mobius (2003), for more detailed discussion.

[289] See: www.apacs.org.uk/media_centre/press/06_31_07.html.

[290] Source: Comscore (2007).

[291] Source: Comscore (2007): In December 2006 Google and Microsoft sites had 25.7 million visitors and eBay was third with 20.9 million.

[292] Nielsen/Netratings (March 2007).

10.13. These marketplaces have had a significant impact on internet shopping. Their advent has greatly facilitated the trade for certain products, such as niche and second hand items, by exposing the listing to a large number of potential buyers at low cost. Online auctions have improved people's ability to sell unwanted items easily. One estimate is that that this could be worth a few thousand pounds per household if they sold all their unwanted possessions.[293]

10.14. Businesses can use the market place as a virtual shop front, reaching millions of consumers without the need to establish their own website or high street shop. Some organisations we spoke to added that online auctions had played a major role in opening up international markets.

10.15. Online auctions have therefore improved or even created markets that did not exist before. These markets offer a virtually unrestricted choice in products for consumers, and increase competition, with eBay listings possibly representing the world's largest inventory.[294]

## Online auctions: Buyer and seller experiences

### Frequency of use and spend

10.16. Our online survey found extensive use of online auctions and marketplaces both as a platform on which to sell and, in particular, to buy. Our focus was on consumers' experiences in buying and selling, but we also asked businesses about how they used online auctions to sell to consumers.

### Individual buyers and sellers

10.17. We found that around half (51 per cent) of our online survey respondents had ever sold via an online market place, although it is important to note that this may overstate usage because online survey respondents were more likely to use the internet than consumers generally (for example, all were internet shoppers). eBay told us and the House of Lords that 68,000 people in the UK, and over 170,000 in the EU, earned at least one quarter of their income from trading on their site.[295]

10.18. Of our online survey respondents, 81 per cent had bought from an online auction site, with 76 per cent bidding on an online auction and 72 per cent buying at a fixed price (again, however, these figures may overstate usage). Of all those online auction shoppers, 65 per cent shopped on them regularly (at least once every month or two); and over half (55 per cent) had spent over £100 in the 12 months to November 2006.

### Business users

10.19. Of respondents to our business survey, 17 per cent had sold via an online auction. Businesses selling online for less than two years were more likely to sell via online auctions – either through competitive bidding or as fixed price sales.

10.20. The main reasons these businesses gave for using online auctions were 'to reach a wider audience' (49 per cent), and to 'sell off old stock' (24 per cent), with only five per cent citing 'cost/cheaper to use an established system' as a reason.

[293] Centre for Economics and Business Research, in: Times Online 'EBay-nomics boosts British households', 15 August 2005.

[294] Mintel, Home Shopping March 2007.

[295] eBay (2006).

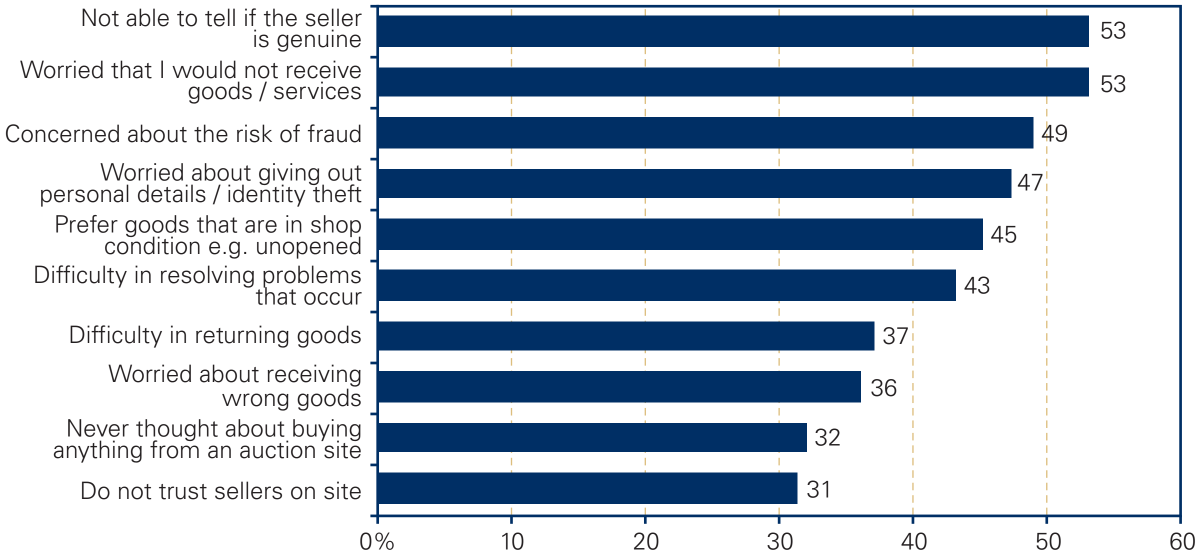
## User attitudes

10.21. There is evidence that the attractions of online auctions to users are more than simply availability and price. Bidding on an auction site may provide a different experience from that of merely purchasing products on the internet. It has been suggested that for some the excitement of an auction may replace the satisfaction of the bricks and mortar shopping experience.[296]

10.22. In our focus group those who shopped on an online auction site on a regular basis said that in some ways it was 'addictive' and that the thrill of beating someone in an online auction was a real 'buzz' which kept them coming back and shopping more.

10.23. However, despite the profile of online auctions and their apparent widespread use by respondents to our survey, it was clear that many people we surveyed had concerns about using them. For those who had never used them, the main reasons related to trust and security fears (Chart 10.1).

**Chart 10.1: Top ten reasons for not buying from online auction sites**



Source: OFT Consumer online survey

Base: All respondents who have never bought from an online auction

10.24. Participants in our focus groups also felt using online auction sites was generally more risky than using other sites to purchase online. As a result, only respondents who were more familiar with the internet or with online shopping used auction sites with any degree of frequency. Indeed when choosing between auction sites, trust also appeared to be the key issue, with the two main factors cited by respondents being a site's reputation/feedback system on sellers (40 per cent), and the reputation of the site itself (24 per cent).

[296] See the Consumer Attitudes Review at Annexe E.

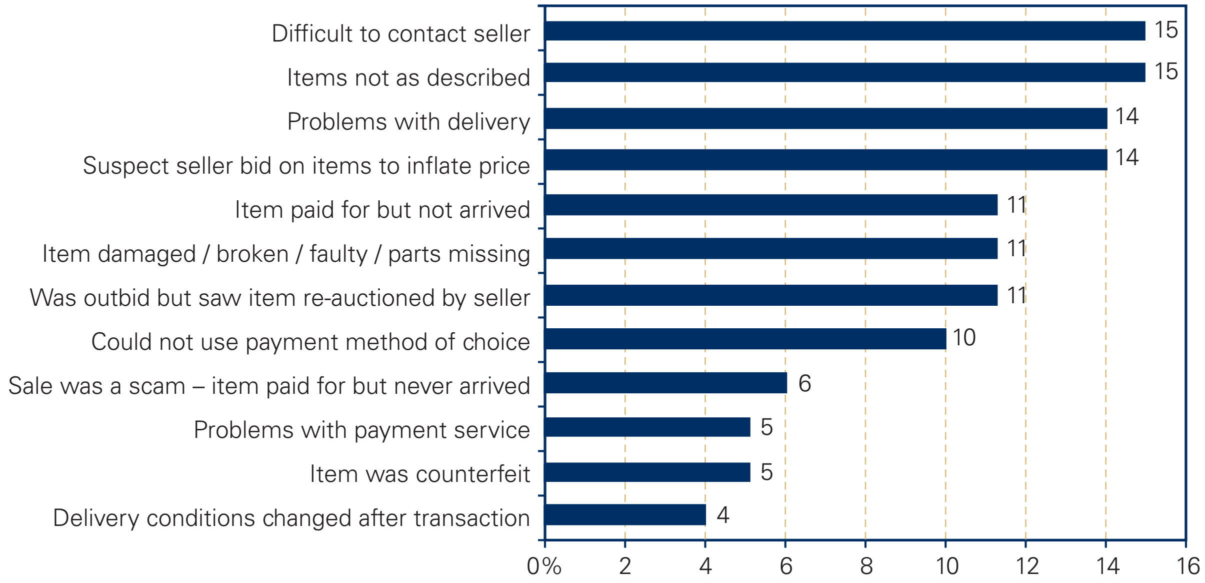
## Problems experienced

10.25. We also found that just over half (52 per cent) of our online survey who had shopped on an online auction site claimed to have experienced a problem when doing so in the past year. Taking the most recent example, in 65 per cent of cases, the buyer had been bidding for the item, while in 30 per cent of the cases they had been buying it at a fixed price.

10.26. Of those who had experienced problems buying from an auction, only 26 per cent had bought from a business, while 60 per cent stated that it occurred with a private seller (14 per cent did not know). This implies that consumers may be more likely to experience a problem when buying from a private seller, although the uncertainties in identifying businesses in online auction sales (discussed below) mean care is needed in interpreting this finding.

10.27. The range of problems cited was diverse (see Chart 10.2), although it is important to note that some responses related to buyers perceiving that there had been a problem.[297] While no single issue dominated, a number of distance selling issues were reported more than other problems. The three most commonly reported problems were 'the seller was difficult to contact' and 'product not as described' (both 15 per cent), followed by 'problems with delivery' (14 per cent).

**Chart 10.2: Problems most commonly experienced or perceived by buyers in past 12 months[298]**



Source: OFT Consumer online survey

Base: All respondents who have bought items from an online auction

10.28. However, another issue that emerged, which was less apparent for internet shopping generally, was that of perceived deception. In some cases, this related to suspected manipulation of the bidding process itself, such as the seller bidding to inflate the price ('shill bidding'). In other cases, buyers suspected the sale itself was a scam or that the goods were counterfeit.

[297] Also, in some cases, the problems cited may not, in fact, have been a problem. For instance 'was outbid but saw item re-auctioned by seller' may reflect instances of people selling an item again if the winning bidder did not pay for it, or if sellers had more than one of the same item to sell.

[298] Figures rounded.

10.29. Empirical studies suggest that the reputation systems operated by auction sites, though not perfect, may provide a reasonable guide to consumers as to whether sellers are reputable. We know from these studies that a good reputation is valuable on eBay at least (see Annexe F). We also note that some commentators have claimed that sites can profit from scams and sales of counterfeit products on their website. Sites, on the other hand, have emphasised that they have a commercial incentive to create an effective and safe market and trust in them would be undermined if manipulation was widespread.

### How buyers reacted to problems

10.30. For the most recent problem that buyers experienced when buying through an online auction, the median value of items involved was £35, which was lower than the median value of problems for the rest of internet shopping at around £55. This difference may reflect the nature and value of products typically bought through online auctions, many of which are second hand. Certainly the types of products for which problems were experienced differed: clothes/shoes (ten per cent), computer/printer components/supplies (nine per cent) and DVDs (eight per cent) for online auctions, compared to electrical items (27 per cent), books, clothes or DVDs (eight per cent respectively) for internet shopping generally.

10.31. Another indication of the significance of a problem is whether or not consumers complained when they experienced a problem. We found that 38 per cent of those who experienced a problem whilst buying from an online auction had not complained. They gave two main reasons in similar measure: 33 per cent 'could not be bothered'; and, for 31 per cent, the value was too low for the effort.

10.32. However, most (62 per cent) consumers had complained. Half of those who complained (49 per cent), had turned to the trader or seller; 23 per cent to the auction site; and 12 per cent to the operator of the payment system. In 52 per cent of the cases where buyers had experienced a problem buying on an online auction site, it had been resolved to their satisfaction. But ten per cent were still trying to resolve it and 38 per cent had given up.

10.33. In summary, while most transactions are completed successfully on online auctions, it would appear that many people have worries about using them. While there are millions of successful transactions, a relatively high proportion of users we surveyed claimed to have experienced problems – typically related to contact with the seller, items not as described, problems with delivery and perceived deception. Although the average value of the items was quite modest and a high proportion of buyers did not complain, of those that did only half achieved a satisfactory conclusion. These findings underline the potential importance of consumer protections for online auction users. We therefore now turn to the regulatory protections available.

## Regulatory issues

10.34. Online auctions represent another means of trading over a distance and therefore raise many of same distance-related selling issues we address in this report. However, they also introduce some new issues for consumer protection on the internet.

## The DSRs and online auction sites

10.35. Whether the DSRs apply is determined by the nature of the transaction. For most types of transaction, the situation is clear:

- The DSRs **do not apply to Business to Business (B2B) sales, Consumer to Business (C2B) sales or Consumer to Consumer (C2C) sales** – whether or not these are on auction sites.
- The DSRs **do generally apply to fixed price Business to Consumer (B2C) sales** on online auction sites.[299]

10.36. However, the DSRs do not apply to distance contracts which are 'concluded at an auction'. The DSRs (and the DSD where this exemption originates) do not define what is meant by 'at an auction'. As set out in Box 10.1 above, there is debate as to whether internet auctions are 'auctions' at all and whether a contract entered into in the course of, or following, an online auction can be said to be 'concluded at an auction' in the way that the writers of the Directive envisaged. This difficulty may be because the Directive predates the current popularity of internet auctions.

10.37. The DTI have recently confirmed that they consider that the DSRs do not apply to internet auctions of the type under consideration in this study[300], although as yet there is no UK case law to confirm this position. However, in other member states the exemption has been held not to apply.[301]

10.38. As discussed above, the European Commission is currently reviewing the DSD as part of the review of the consumer acquis and has highlighted the treatment of online auctions as an issue that needs to be addressed.

## Business sellers – information requirements

10.39. The ECRs impose various information requirements upon businesses selling on the internet, including at internet auction sites. These information requirements apply both to the auction company providing the auction platform and also to individual businesses trading on the auction platform.

10.40. Unlike the case with the DSRs this information must be provided whether or not the buyer is a consumer or another business, and whether or not the items are listed for sale using an auction or a fixed price format. It is a requirement of the ECRs, for example, that a business seller using an online auction must make available to buyers his name, geographic address and details, including his email address.[302]

[299] Regulation 3 (1).'One-off' sales are unlikely to be caught. The contract must be made under an organised distance sales or service provision scheme for the DSRs to apply.

[300] See: www.dti.gov.uk/files/file39758.pdf

[301] There has been a case in Germany considering the application of the Distance Selling Directive to a contract concluded following competitive bidding on eBay. In this case, the claimant dealt in jewellery as a business. He sold a diamond bracelet on an eBay auction to a consumer who, on receipt and inspection, wished to exercise cancellation rights. The German court concluded that the consumer was entitled to exercise cancellation rights under the Directivie (BGH (DE) 03, Nov. 2004 VIII ZR 375/03).

[302] This information must be provided in a form and manner which is easily, directly and permanently accessible. The electronic mail address must make it possible to contact him rapidly and to communicate with him in a direct and effective manner (Regulation 6(1)). Other requirements include the indication of which relevant codes of conduct the business adheres to. See Regulations 6-11 for other requirements.

10.41. However, this regulatory requirement is not always being complied with. This may make it difficult for consumers to know who they are dealing with, and, in some cases, whether or not the particular seller is selling in the course of a business. Obviously this could seriously affect their ability to exercise their rights.

10.42. Our survey of Trading Standards Services also identified that there were implications for enforcers of consumer rights, with one respondent stating that:

> *'…the anonymity of the internet causes problems in identifying the legal entity to be investigated and what that entity is – e.g. on [online auction sites] you can have private individuals, individuals selling as a hobby/as a second income, businesses selling as individuals, and shops…'.*

10.43. However, eBay told us that they were looking at technological solutions whereby sellers' registration details would be provided to buyers automatically.

## The liability of online auction hosts

10.44. Even traditional auctioneers, who act as agents of the sellers, are rarely responsible to buyers for the quality of the goods or the accuracy of the descriptions. For online auctions this is even less likely to be the case. Not only do the platforms not act as the seller's agent, they do not describe the goods or take possession of them.

10.45. Indeed, under the ECRs, online auction hosts have no civil or criminal liability for illegal or infringing content which has been uploaded by sellers on to their sites where they:

- do not have actual knowledge of unlawful activity or information and, where a claim for damages is made, they are not aware of facts or circumstances from which it would have been apparent that the activity or information was unlawful; or
- upon obtaining such knowledge or awareness, they act expeditiously to remove or to disable access to the information.[303]

10.46. Under the ECRs, online auction sites have no obligation actively to monitor content, nor to ascertain if illegal content is being posted on their site – although eBay told us that it uses 'leading edge technology' to assist in finding and taking down listings offering certain types of prohibited items. However, for a member state to impose a monitoring obligation would be incompatible with the E-Commerce Directive.

10.47. The major online auction sites typically include advice on their sites that they are not responsible for the contents of the listings. For instance, they state that they are venues only, and do not accept liability for the quality, safety or legality of the items listed, nor for any losses to buyers or sellers arising from sales. However, some auction sites also offer protection for buyers – for instance, to pay up to a certain amount if they do not receive an item or it differs significantly from what was described.

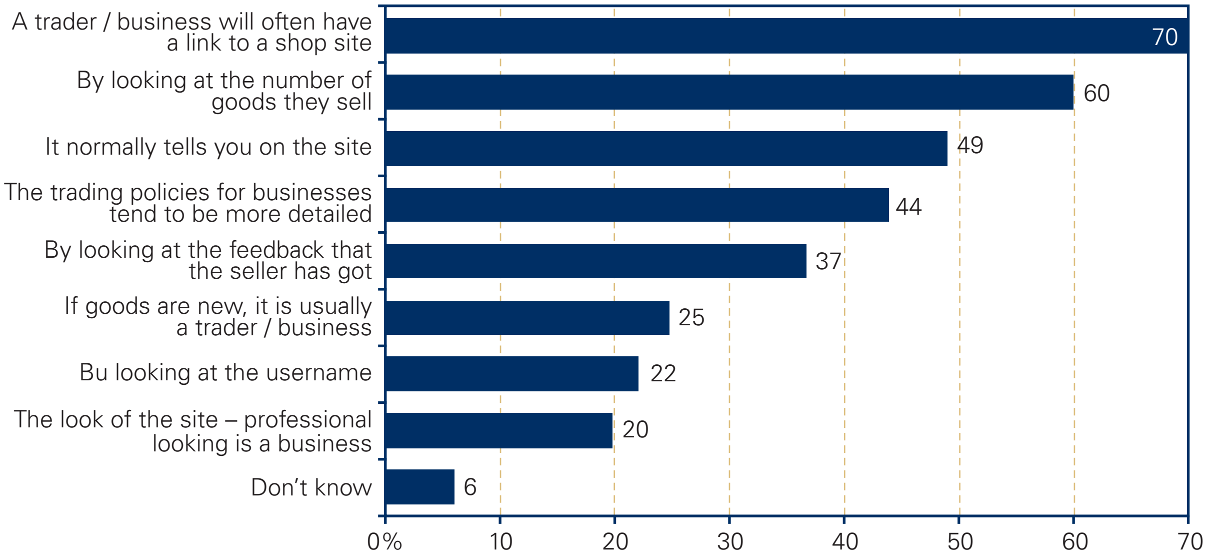
## Is a seller selling 'in the course of business'?

10.48. As outlined above, whether a seller on an online auction site is a business or not is a key question in applying consumer protection law.

[303] Regulation 19 ECRs

10.49. It also seems clear that the status of the seller matters to consumers. We found that 60 per cent of online survey respondents who had bought from an online auction agreed that they prefer to know if the business is a trader or private seller. Furthermore, 62 per cent disagreed or strongly disagreed with the proposition: 'I have more confidence when buying from a private seller than a trader/business', and 65 per cent had tried to identify whether or not a seller on an auction site was a business. However, it also seemed that consumers had no fixed way of telling whether the seller was a business – the main indicators they cited included whether the seller had a link to a shop, the number of items they were selling, whether the seller said it was a business, and the level of detail in their trading policy (see Chart 10.3).

**Chart 10.3: How do buyers try to tell if the seller is a business or a private seller?**



Source: OFT Consumer online survey

Base: All respondents who have bought items on an online auction

10.50. While it is good that many buyers try to assess the status of the seller, many of the ways they do so offer no certainty – for instance, the number of goods a seller sells is not a perfect measure. Furthermore, we again found variation at the time of writing in the advice being provided by online auction sites to their users. In some cases, we could find no advice (at least on the basis of a short search), in others we found suggestions for a range of indicators to judge seller reliability, but no detailed advice on how to judge whether a seller should be considered a business. This may in part reflect the complexity of the law in this area.

10.51. Better compliance with the ECRs would aid consumers in this assessment. Under separate regulations[304], businesses advertising goods for sale must make it reasonably clear that the goods are being sold in the course of a business. These regulations do not apply to sales by auction (and so there is similar uncertainty in application to internet auctions as with the DSRs) but they clearly do apply to 'buy now' type sales. The CPRs impose similar obligations, and make no exemption for sales by auction.[305]

[304] Business Advertisements (Disclosure) Order 1977

[305] Under the UCPD ( Annexe 1 Practice 22) falsely claiming or creating the impression that the trader is not acting for purposes relating to his trade, business, craft or profession, or falsely representing oneself as a consumer is a commercial practice which will be considered unfair in all circumstances. Regulations implementing the UCPD will come into force in the UK in April 2008. See Chapter 12.

10.52. But sellers themselves may be unclear about their status. Online auctions are popular with 'hobby' type sellers. There is always likely to be a grey area, where a seller may be on the margins of being a 'business' and, indeed, their status could change over time depending on their activities.

10.53. HM Revenue and Customs (HMRC) recently produced guidance on the issue of internet trading for tax purposes. The guidance is set out on a page[306] of the HMRC website which takes sellers through the legal tests applied to determine whether a seller is liable for income tax. These legal rules have been developed over a long period by the courts and are known as the 'badges of trade'. They take account of such issues as the frequency of transactions, whether a transaction was entered with a view to profit and the nature of the goods. A full list of the nine badges can also be found on the HMRC website.[307] HMRC also provide a list of examples[308] which includes one (Example 6) on internet auctions.

10.54. Although this advice relates specifically to tax issues, we can see a benefit in sellers being provided with similar guidance as to when obligations may arise under consumer protection laws. Currently, however, advice on this does not seem to appear prominently on all online auction sites.

## Other issues

### Shill bidding

10.55. We described earlier in the Chapter that a lack of trust in sellers put many potential users off online auctions. We also found that some buyers suspected that they had suffered a con when buying through competitive bidding. This underlines the importance of generating and maintaining trust in bidding processes.

10.56. As discussed at para 10.28, shill bidding was the main form of deceptive practice suspected in our online survey (13.6 per cent). This is where a seller makes strategic bids, for example from an additional anonymous account or by an associate. Undisclosed shill bidding is illegal[309] and most auction sites expressly prohibit it.

10.57. eBay told us that they provided online tutorials to educate users about shill bidding, used behavioural analysis and account linking technology to track suspicious bidding patterns and took action wherever necessary to prevent it – for example, by suspending users or restricting their ability to bid on future auctions. However, they could not provide us with detailed data on the extent to which there was suspicious behaviour.

10.58. We wish to pursue further with all online auction hosts how they are ensuring that users of their sites can have confidence in the bidding process.

[306] www.hmrc.gov.uk/guidance/selling/income.htm.

[307] www.hmrc.gov.uk/guidance/selling/badges.htm.

[308] www.hmrc.gov.uk/guidance/selling/examples.htm.

[309] The Fraud Act 2006, which came into force in January 2007, makes it an offence for a person to commit fraud by false representation where the representation is made dishonestly and with the intention of making a gain for himself or another. Under section 57(4) of the Sale of Goods Act 1979, it is not lawful for a seller to bid himself or to employ any person to bid on his behalf at a sale by auction unless the auction is notified to be subject to such a right. A sale contravening this section may be treated as fraudulent by the buyer.

### Scams and counterfeit goods

10.59. Complaints and enquiries data from Consumer Direct suggest that while internet auctions have proportionately fewer complaints in some areas, misleading claims and omissions may be a particular issue for online auction sites, with a higher proportion of such complaints relating to sales on internet auctions than over the internet generally (Table 10.1).

**Table 10.1: Top 5 types of complaints recorded (2006)**

| Complaint type | All complaints | Internet | Internet auction |
|---|---:|---:|---:|
| Defective goods | 41% | 38% | 38% |
| Delivery/Collection/Repair | 7% | 23% | 17% |
| Misleading claims/Omissions | 9% | 11% | **26%** |
| Substandard services | 24% | 14% | 6% |
| Prices | 4% | 3% | 1% |

Source: Consumer Direct

10.60. Chapter 8 also noted that a high proportion of internet-related investigations by TSS covered counterfeiting, and Trading Standards officers told us that that they received a lot of complaints about fake branded goods which were listed as genuine on online auctions. The issue of counterfeiting was highlighted for attention by the recent Gowers Review[310] and an additional £5m this year has been made available to TSS following additional Trading Standards powers in respect of copyright that commenced on 6 April 2007.

10.61. The issue of counterfeiting is clearly a matter of concern to rights holders in particular. One group told us that the internet had dramatically reshaped the marketplace for counterfeits in the UK by increasing the level of their international supply into the UK and suggested that the emergence of internet auction sites had added a new layer of distribution in the counterfeit marketplace.

10.62. As discussed above, under the ECRs, online auction sites have no obligation to monitor content actively, nor to ascertain if illegal content is being posted on their sites. We were told that it would be unrealistic to expect online marketplaces to monitor for counterfeits both because of the huge number of trades conducted on their sites and because they did not have the necessary expertise to identify fake items which are never in their possession.

10.63. Online auctions also told us that they were dependant on Rights Owners to help them deal with counterfeits. The largest UK site, eBay, states[311] that it is 'committed to help protecting the intellectual property rights of rights owners…'. Its Verified Rights Owner (VeRO) Programme, enables rights owners to report listings that have potentially infringed their rights. More recently, for some items reportedly favoured by counterfeiters, eBay told us that it had eliminated the ability to list these items with one or three-day auction durations and now requires additional seller verification and places additional restrictions for people selling these items cross-border.

[310] Gowers (2006).

[311] See pages.ebay.co.uk/vero/index.html.

10.64. While these initiatives have been in place for a relatively short time, eBay stated that the number of reports from Rights Owners had significantly decreased as a result. However, this raises concerns regarding displacement if these traders are moving to other auction sites to sell counterfeit goods. Hence, an industry-wide approach to the issue of counterfeiting is likely to be required.

10.65. It was not the intention of this study to assess the effectiveness of the anti-counterfeit measures adopted by the industry. However, as the anonymity and international scope of the internet proves attractive to counterfeiters, it is important that the industry and enforcers work together to reduce the number of counterfeits being marketed and to remove those that are from sale quickly.

## Next steps

10.66. We want to work with the online auction sites and others to ensure that sellers on such platforms know how to comply with their legal obligations to consumers. Our strategy to improve consumer and business awareness will include advice in this area as well as how to deal with deceptive practices. For instance, while buyers are likely to find it hard to spot practices like shill bidding, any future advice on using auctions might for instance suggest that shoppers consider how much they want to pay for the item and whether the item is available elsewhere and avoid getting too carried away when bidding (bearing in mind that some told us that they found bidding addictive). It could also encourage them to report suspicions of manipulation to auction hosts.

10.67. We will encourage sellers to self-assess to ensure they are meeting their obligations. We want to investigate further how businesses selling via online auctions can be more clearly identifiable to buyers. Where businesses are not complying with regulatory requirements, and there is clear evidence of consumer detriment, we will take appropriate action to ensure that this is addressed.

10.68. We also want to investigate how the online auction sites are addressing issues like counterfeiting and sellers bidding up their items.

# 11 CROSS-BORDER TRADE

## Summary

Although a higher proportion of consumers told us that they had bought online from non-UK websites than other surveys have found, many are also unsure how to tell whether a site was based in the UK. For those consumers who do not buy online from other countries, this is either because it does not occur to them, or because of concerns about problems they might encounter – especially with delivery and communication with the trader.

Although 37 per cent of UK businesses told us that they aimed to sell to foreign consumers, the rest do not. Their reasons included that it would not be suitable for their products, concerns about delivery costs, and to a lesser extent the regulations they would need to comply with.

By value, 92 per cent of internet purchases by UK consumers are therefore currently from UK businesses. Similarly, UK businesses surveyed estimated that 93 per cent of their online sales were to UK consumers. Where consumers do buy from websites abroad, and businesses sell abroad, the other party involved is most likely to be based elsewhere in the EU. While there is a lack of reliable and comparable statistics on the volume and value of cross-border internet trade, UK internet shoppers seem relatively less willing to shop online outside the UK compared to other European consumers, and more likely to be concerned about doing so.

Businesses and consumers do not appear much more likely to experience problems with foreign than domestic internet transactions, and those problems which do occur most often relate to deliveries. Although consumers' awareness of their rights for international purchases is low, those experiencing problems when buying from abroad are likely to complain. Our evidence did not show a great difference in the relative likelihood of cross-border and domestic complaints resulting in resolution.

Internet shoppers' rights within the EU share a common framework, which includes requiring e-tailers within the EU to provide consumers with a minimum seven-day cancellation period in which to cancel the contract without penalty and without giving any reason. This, along with measures such as the Consumer Protection Cooperation (CPC) Regulation, should help consumers to buy with confidence online from anywhere in the EU.

However, outside Europe, the protections for consumers are less well established. Some international agreements and networks exist, although these have tended to address general threats to internet users, such as spam and scams. These partnerships could provide a valuable basis on which to focus more attention on protecting consumers' rights when buying from online traders.

## Next steps

In earlier chapters we consider the importance of raising consumers' awareness of their rights. This should include raising awareness of what to look for to identify the location of a trader, as well as how to handle any problems that arise when buying from abroad. We will also explore with enforcement partners how to improve international co-operation in addressing problems arising from cross-border shopping.

## Introduction

11.1. This chapter addresses the subject of cross-border internet shopping, largely from the perspective of UK consumers and businesses. It examines the extent of cross-border online trade, as well as how consumers and businesses feel about buying and selling abroad. It looks at the problems which they experience, and the effectiveness of various methods of solving them. It then outlines the regulations governing cross-border transactions, as well as the mechanisms in place for enforcement of the regulations.

## The extent of cross-border internet trade

### To what extent do UK consumers buy from abroad?

11.2. Despite expectations that the internet would bring about a global marketplace, most available evidence suggests that cross-border purchasing by UK consumers is relatively modest:

- A 2006 Eurobarometer survey reported that only seven per cent of UK consumers had purchased goods or services via the internet in the last 12 months from a seller/provider located in another EU country. On this measure, the UK was close to the EU average of six per cent of citizens who had made a cross-border internet purchase from within the EU and three per cent from outside.[312]
- A leading payment card company also told us that as a proportion of all online payment card spend by UK consumers, 92 per cent was with UK suppliers; with only five per cent spent on products from EU suppliers and three per cent from suppliers in the rest of the world.

11.3. In our telephone survey of consumers, nearly half (47 per cent) said they had made at least one purchase from a non-UK site within the last 12 months, but this may, in part reflect uncertainty over what a 'non-UK site' is.[313] For instance, over a third of internet shoppers (34 per cent) said that they were not able to tell whether or not a business operating a site was based in the UK.

11.4. Furthermore, the most popular way of checking whether a site was in the UK was to see if the website address was 'co.uk' (cited by 41 per cent). Likewise, most participants in our consumer focus groups assumed that a 'co.uk' in the address indicated a UK site, although they also looked for clues like language, prices in pounds, and a UK address or phone number.

11.5. However, Nominet told us that about five per cent of '.co.uk' addresses were registered to overseas locations, of which the United States was the most popular. Conversely a business with a '.com' domain may be based in the UK or outside the UK: there is no geographical limitation in its use, so it is not possible to know the location of a business from its domain name. This underlines the need for consumers not just to rely on website addresses as a sign of where a trader is based, but also to look for this information on the site if they have decided to buy.

[312] European Commission (2006a).

[313] It may also reflect respondents including purchases such as foreign holiday bookings and car hire.

### To what extent do UK businesses sell abroad?

11.6. Our survey suggested a willingness on the part of many UK businesses to sell to non-UK consumers. It found that 37 per cent of online businesses (and 75 per cent of music retailers) said that their website, or the one they used, was aimed at selling to individuals outside the UK. Of these businesses, most were selling to the rest of the EU (91 per cent) compared to the US (78 per cent) or the rest of the world (84 per cent).[314] Nevertheless, 63 per cent of online businesses we surveyed were not aiming to sell abroad.

11.7. By value, cross-border online sales also represent only a small proportion of overall online sales. An ONS survey of UK businesses found that, in 2005, for every £100 worth of goods and services they sold online to both businesses and consumers, £82 was to the UK, £9 was to the rest of the EU and £9 was to the rest of the world (it was not possible to estimate what proportion of these sales was to consumers only).[315] However, online traders in our survey estimated that, in practice, their sales to UK consumers averaged 93 per cent of all their online sales.[316]

## Consumer and business attitudes to cross-border internet trade

### Consumers' attitudes

11.8. A 2002 MORI survey for the Department of Trade and Industry showed that 'lower prices' was the main reason given by respondents for buying across-borders, together with convenience, the variety of goods available, including items not available in the UK. However, the same DTI survey found that 53 per cent of UK adults said they 'would not use the internet to buy goods or services abroad,' compared to 31 per cent who said they would be inclined to do so.

11.9. There is a lack of reliable comparative data on cross-border flows – an issue the OECD has sought to address.[317] However, there is some evidence that UK consumers may be more reluctant to buy from across borders than some of their European counterparts. For instance:

- in 2006, the European Commission found that Denmark, the Netherlands, and Sweden all had broadly similar proportions to the UK of consumers buying online from businesses in their own country, but two to nearly three times the proportion of consumers buying online from other EC countries[318]
- in our survey of ICPEN member countries, the Belgian federal enforcement agency, Directorate General for Enforcement and Mediation told us that 60 per cent of online purchases by consumers in their country were from foreign websites; and the office of the Norwegian Consumer Ombudsman said that half of all online purchases in their country were from abroad.

[314] European Commission (2006b), asking a different question, found that 23 per cent of UK businesses were currently making cross-border sales (on- or offline sales not including sales at trader premises) to one or more other EU countries, compared to an EU25 average of 29 per cent).

[315] Office for National Statistics (2005b). The results of this survey exclude businesses with fewer than ten employees.

[316] European Commission (2006b) found that of those UK internet retailers who were making cross-border sales to consumers within the EU, these sales were on average 16 per cent of all their sales.

[317] OECD (2005a) gives a summary of comparative data on international e-commerce from the OECD. It also identifies some of the challenges involved in measuring e-commerce, particularly when attempting to draw international comparisons. This is also discussed in more detail in OECD (2005b).

[318] European Commission (2006a).

11.10. We found that the main reason why UK consumers did not buy online from non-UK businesses was simply that they had not thought about it, or not needed or wanted to (45 per cent). 'Delivery fees too expensive' was cited by 15 per cent. Lack of confidence was another factor: 14 per cent said that they were 'concerned about security issues/other countries' security policies'; and eight per cent that they were 'afraid the product would not arrive'. Only five per cent said that it was because they thought the trader would be harder to contact if there were a problem.

11.11. In our focus groups, more confident online shoppers were happy to buy from abroad if the site had a contact name and an address in the UK. However, they also cited concerns about the cost of communicating abroad over the telephone and possible language barriers:[319]

*'You would not be wary because it was not a British site specifically, you would be wary about the ability to return the item, communicate with the staff there…'* (Internet shopper, Fife, younger)

11.12. These attitudes reflect survey results from the EC, which suggest UK consumers are marginally more likely to be concerned about cross-border shopping than their counterparts in other EU countries:[320]

- 56 per cent of UK respondents said they would be less confident buying goods or services online from providers in other EU countries, compared to 45 per cent of respondents across the 25 EU countries
- Three quarters (75 per cent) of UK consumers saw greater risk of falling victim to scam or fraud from EU cross-border shopping, compared to two thirds (68 per cent) of consumers across the 25 EU countries
- 73 per cent of UK consumers foresaw a greater chance of delivery problems compared to 66 per cent of respondents across the EU

## Business attitudes

11.13. International bodies we spoke to noted that businesses' desire to promote sales to other countries seemed lower than some commentators had expected in the early days of internet trading.[321] The majority (57 per cent) of EU consumers had not seen a cross-border advertisement in the past year,[322] suggesting that EU firms are generally not promoting their business to the cross-border market as effectively as they might.

11.14. However, we found that most UK businesses were prepared to consider selling to non-UK consumers – especially in the EU and US. In our survey, four in ten (41 per cent) UK businesses not currently selling online abroad were considering selling to the rest of the EU, while three in ten (30 per cent) were considering selling to the USA or to the rest of the world (29 per cent).[323]

[319] However, European Commission (2006a) found that as many as 29 per cent of UK consumers were prepared to make a cross-border purchase in another EU language, in line with the EU average of 32 per cent, suggesting that language may not be a critical issue hindering cross-border shopping in the EU.

[320] European Commission (2006a).

[321] This is not necessarily to say that businesses will refuse to sell goods to those in other countries who wish to buy them, but rather that they appear not to promote their products actively to the international market as much as they might.

[322] European Commission (2006a).

[323] A 2006 survey (European Commission (2006b)) found that the same proportion – 40 per cent – of UK businesses using the internet/e-commerce for retail, but with no experience of cross-border sales, were prepared to sell abroad (compared to an EU25 average of 37 per cent).

11.15. Our business survey also suggested that the barriers to businesses' selling across borders were mainly practical rather than related to uncertainty about regulations. For example a quarter of all businesses not considering selling abroad (46 per cent of travel companies) said the reason was that international trade was inappropriate to their product. And 14 per cent said delivery costs were the problem (31 per cent of electrical retailers). Only eight per cent cited weak understanding of law as a barrier.

11.16. However, in our meetings, trade bodies (which were mainly representing larger businesses) and businesses, cited regulatory barriers such as variations in cancellation periods as a factor that potentially impeded cross-border trade. Some cited concerns about the burden placed on them by existing law which requires them, in certain circumstances, to comply with the mandatory consumer protection laws of each of the countries they sell to.[324] They were concerned at the prospect of future developments in this area, whereby such contracts may be governed in their entirety by the law of the consumer's residence.[325]

11.17. These views more closely echo those of a 2006 EC survey[326] which found, for example, that 78 per cent of UK businesses (compared with 51 per cent of EU25 businesses) considered that different national laws regulating consumer transactions were an important or very important obstacle to cross-border sales. It also found that UK businesses were more likely than the EU25 average to see important or very important obstacles to cross-border trade in, for example, different fiscal regulations (76 per cent of UK businesses versus 51 per cent of EU25 businesses), cross-border delivery costs (73 per cent versus 46 per cent), and difficulties in resolving complaints and conflicts (78 per cent versus 51 per cent). However, the fact that these results seem to emphasise barriers more strongly than our own survey findings most likely stems from the fact that responses to our survey were unprompted, whereas the EC's were prompted.

## Consumer and business experiences of cross-border internet trade

### Problems experienced

11.18. The European Consumer Centres (ECC-Net) is an EU cross-border B2C advice and dispute resolution service. Its 2005 report[327] identified an increase of 74 per cent in the total number of complaints and disputes recorded across its whole network. There could, however, be a number of reasons for this.[328] Our survey findings suggest that businesses and consumers are no more likely to experience problems with foreign than domestic internet transactions.

11.19. Ten per cent of online shoppers who had experienced problems when buying online in the last 12 months said that the most recent problem had been when shopping from a non-UK site. This is similar to DTI survey data that 13 per cent of internet shoppers had been in a position to seek redress from one or more non-UK traders or suppliers in the previous year.[329] This suggests that the proportion of problems experienced from cross-border trade is similar to the apparent distribution of spend (eight per cent being cross-border).

[324] Contracts (Applicable Law) Act 1990 implementing the Rome Convention into UK law.

[325] See the Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I), Brussels, 15.12.2005 COM (2005) 650 final 2005/0261 (COD). For the response of the FSB, see www.fsb.org.uk/news.asp?REC=3883.

[326] European Commission (2006b).

[327] See: ec.europa.eu/consumers/redress/ecc_network/eur_online_marketplace_2005.pdf.

[328] Reasons could include the recent expansion in the size of the network, increased publicity and the ongoing growth in internet shopping (including cross-border).

[329] DTI/YouGov (2005). Note that the base for this was all cross-border purchases of which only 70 per cent were online.

11.20. Likewise, business respondents to our survey selling across borders also said that their overseas sales were no more likely to generate complaints from consumers than UK sales: 55 per cent said they were as likely, 13 per cent said they were slightly or much more likely, and 17 per cent said they were slightly or much less likely.

11.21. The most common complaint type concerned problems with delivery, which were the cause of 46 per cent of all internet shopping complaints and disputes reported to the ECC-net in 2005. Problems relating to the quality or condition of the product represented the second most common area, with 25 per cent of complaints. Problems regarding price and payment, contract terms and redress accounted for eight per cent, eight per cent and five per cent of complaints, respectively.[330]

11.22. The numbers in our surveys were too small to be sure about the nature of the problems experienced by consumers buying across borders. However, for the 23 per cent of UK businesses that had experienced problems when selling to non-UK consumers, by far the most frequently cited problem related to unreliable delivery (37 per cent: base 54). Many other issues were raised by much smaller numbers of businesses, of which the most frequent were problems with different consumer rights (six per cent), taxes/import duties (four per cent), and language differences (four per cent).

## Complaints and redress

11.23. When they do experience cross-border problems, many consumers seem willing to complain. DTI found that only 11 per cent of those in position to seek international redress had not done so. For those who did not complain, the value of purchases was lower compared to those who did, and their main reason for not doing so was that the claim was too little to worry about (25 per cent).[331]

11.24. According to ECC-Net, of the complaints they received in 2005, 43 per cent had been resolved through discussions with the consumer, 17 per cent with the help of a third party; and 13 per cent through voluntary settlement. However, 23 per cent had not been possible to resolve.[332] Our consumer survey found that a similar proportion – one in five (20 per cent) – of all consumers who reported experiencing a problem shopping from a UK or foreign website had given up trying to resolve it.

11.25. Given the difficulties some consumers had had in achieving redress in cases of problems shopping online from abroad, an alternative might be found in the existence of voluntary code and self-regulation schemes for businesses. However, trans-national code schemes have failed to take root to date:

- Global Trustmark Alliance[333] was set up in 1999 to bring together domestic trustmark organisations and ultimately develop a cross-border code of practice but it seems to have made little recent progress.
- The EC set up the Euro-label Trust Mark in 2001, but this remains small scale and largely concentrated in Germany and Austria.

[330] ec.europa.eu/consumers/redress/ecc_network/eur_online_marketplace_2005.pdf

[331] DTI/YouGov Cross-border consumer redress research (stage 1: phase 2), October 2005

[332] ec.europa.eu/consumers/redress/ecc_network/eur_online_marketplace_2005.pdf

[333] www.globaltrustmarkalliance.org

- BEUC, UNICE and the European Commission, through the 'e-confidence project', tried in 2001 to establish a set of pan-European standards for e-commerce self regulation.[334] However, it failed to receive sufficient backing and the initiative was effectively wound up in 2004.[335]

11.26. A 2006 study found that, though online trustmarks were evident in most European countries, relatively few traders had been approved by them. It identified cultural and linguistic barriers to the establishment of one single scheme for Europe.[336] The NCC also concluded that voluntary self-regulation is inappropriate for cross border consumer protection, because it is too hard to achieve uniformity and ensure compliance.[337] Given the slow take up of domestic code schemes (see Chapter 7) and the additional difficulties faced by cross-border schemes, they seem unlikely to be a significant feature for internet shopping in the immediate future.

## Consumer rights when buying online from other countries

11.27. Chapter 6 noted consumers' low awareness of their rights when shopping online in the UK, and this extends to the cross-border market. DTI research found that, of UK consumers interviewed in 2005, only five per cent believed they were fully aware of their rights as a consumer in the international marketplace and 31 per cent were partly aware of their rights, but 45 per cent did not understand their rights at all.[338] Moreover, 65 per cent of UK consumers did not know where to get advice about EU cross-border shopping.

11.28. Some participants in our focus groups also said that their uncertainty about legal protection was a barrier to buying from abroad:

*'It always worries me because they are not governed by the same laws…. If something happened you'd hopefully be able to go to someone or some watchdog that oversees it or something over here but abroad not'.* (Non shoppers /lapsed, Newcastle, older).

*'If a company is British as a last resort you can go to the small claims court. I do not know if that is possible for sites located abroad'.* (Internet shopper, Fife, younger)

11.29. This lack of awareness of sources of advice is a pan-European issue: 67 per cent of Europeans do not know where they could get information and advice about cross-border shopping in the Union, while 24 per cent claim that they do.[339]

### Consumers' rights when buying from another country in the EC

11.30. Many of the rights UK consumers have derive from EU measures which ensure a common minimum level of consumer protection rights across Europe. For instance the rights under the DSRs derive from the Distance Selling Directive, which has been adopted across Europe. Thus, for instance, if they buy from a business elsewhere in the EU, they are still entitled to a minimum of seven working days in which to cancel their purchase. Likewise, rights under the Sale of Goods Act 1979 (as amended)[340] derive in part from the Consumer Sales and Guarantees Directive.

[334] BEUC (2001).

[335] European Commission (2004).

[336] Trzaskowski (2006).

[337] Self-regulation: the National Consumer Council's position – www.ncc.org.uk/regulation/selfregulation_position.pdf

[338] DTI (2005b). This research did not focus exclusively on the internet, though the majority of sales were on the internet.

[339] European Commission (2006a).

[340] The Sale of Goods Act 1979 (as amended by the Sale and Supply of Goods to Consumers Regulations 2002 implementing the Consumer Sales and Guarantees Directive) among other things gives rights to consumers if goods fail to conform to the contract at the time of delivery. The amendments also relate to the passing of risk in consumer contracts which has been considered in chapter 5 above (see paragraph 5.26). See "A Trader's guide: the Law Relating to the Supply of Goods and Services", April 2005, at www.dti.gov.uk/files/file25486.pdf.

11.31. A Member State may provide consumer protection above this minimum threshold. There may therefore be some differences in the level of consumer protection across Europe – for example, in the length of the cancellation period in different countries, with some countries granting longer periods than the minimum. As mentioned earlier, the European Commission is currently undertaking a review of consumer protection legislation. One outcome of this may be full harmonisation of cancellation periods across Europe which may create greater certainty (see Chapter 12).

11.32. There is also an international framework in place in relation to the law and jurisdiction applicable to contractual disputes between European consumers and businesses. The Rome Convention[341] and the Brussels Regulation[342] respectively establish which country's laws will apply and which country's courts have jurisdiction to hear claims relating to cross border consumer contracts.

11.33. In broad terms, the intention behind the framework is that European consumers who buy from a business in another EU country which has been marketing its products at them should be able to rely on the mandatory protections of their own country's consumer laws and have the dispute heard before their own country's courts – whatever the business might state on its website. However, the rules are complex and can vary according to the circumstances: consumers are unlikely to find private litigation a viable option, particularly for small value purchases. Examples of cross-border private enforcement for any transactions are therefore rare.

11.34. While it is unreasonable to expect consumers to be aware of all the complexities, the evidence on poor awareness does suggest that consumers should be advised about the key tenets if buying within Europe:

- they are entitled to the minimum requirements of the Distance Selling Directive (including at least seven working days cancellation period) and rights under the Consumer Sales and Guarantees Directive
- if they have problems that they cannot resolve with the trader, they can turn to sources of advice such as Consumer Direct and TSS, as well as to the European Consumer Centres.

11.35. Measures are gradually being introduced to address problems in cross border private enforcement within the EU. From 2009, a European Small Claims Procedure will be in place to help EU citizens to pursue cross-border claims (see Chapter 12).[343]

11.36. In addition to private enforcement, measures have also been put in place within Europe to enable public authorities to take action to ensure that specific consumer protection legislation is upheld. The two key ones are the Injunctions Directive and the Consumer Protection Co-operation Regulation (See Box 11.1).

[341] The Rome Convention applies to all member states within the EU. It has been incorporated into UK law by the Contracts (Applicable Law) Act 1990.

[342] The Brussels Regulation applies to all EU member states except Denmark. The Lugano Convention applies similar rules to the EEA countries of Iceland, Liechtenstein and Norway. The Brussels Regulation was incorporated into UK law by the Civil Jurisdiction and Judgments Order 2001.

[343] See: www.dca.gov.uk/consult/smallclaims/smallclaims.htm.

### Box 11.1: European consumer protection measures

**Injunctions Directive**

Under this Directive[344] the OFT can take proceedings in another EEA country,[345] if a business is harming the collective interests of UK consumers by breaching European consumer protection laws. The OFT has used this power to obtain an injunction against a Belgian company, D Duchesne SA, from sending misleading mail order advertisements to UK consumers.[346]

**Consumer Protection Co-operation Regulation ('the CPC')**

The CPC, which came into force in UK law in December 2006, also gives the OFT and other national consumer protection authorities in Europe greater powers to protect consumers from cross-border breaches of specified consumer protection laws. It creates a network of consumer protection authorities in Europe which are responsible for coordinating the application of the CPC within that country. The OFT is the relevant authority in the case of the UK.

These authorities can call upon each other to supply information about, or to take action against, a trader in their jurisdiction even though the activities of the trader may be causing detriment to the consumers in another Member State. This is described in the CPC as 'mutual assistance'. This is an important new development which could be a powerful tool in the future to address breaches of the regulations by businesses selling online in Europe.

11.37. So far, there have been relatively few cases involving UK enforcers working with European partners to address cross-border internet traders. The continued growth, however, of internet shopping along with new instruments such as the CPC means that more cases may be expected in the future.

## Consumers' rights when buying from another country outside the EC

11.38. Consumers can be less certain of which laws apply and which country's courts may hear claims when they buy products from companies which are not based in Europe. As described above, the use of a '.co.uk' domain name does not necessarily indicate that the business is based in the United Kingdom. Conversely, a business operating in the UK or anywhere else may use a '.com' domain for commercial or other reasons.

11.39. Consumers buying online therefore need to:

- check the website to see where the business is located
- see which choice of law and jurisdiction the internet retailer proposes contracts will be subject to.

11.40. When doing so, they need to be aware that if the website says that the contract will be subject to the laws of the retailer's country and that any disputes will be heard before the courts of that country, it may be difficult and costly to argue that the contract should, in fact, be subject to English law and the jurisdiction of the English courts. This is, however, a complex area and each case needs to be judged on its own facts.

[344] Implemented into UK law as Part 8 of the Enterprise Act 2002.

[345] EEA countries include countries within the European Union together with Iceland, Liechtenstein and Norway.

[346] www.oft.gov.uk/news/press/2004/208-04.

11.41. While there are some international arrangements in place to help protect consumers, most focus has been on working together to address online threats such as crime, security, privacy, fraud, spam and scams. Examples of these initiatives include:

- Council of Europe Convention on Cybercrime (2001)
- London Action Plan – International Spam Enforcement Network
- StopSpamAlliance (an initiative of APEC, CNSA, LAP, ITU, OECD and the Seoul-Melbourne Anti-Spam Group)

11.42. Beyond the EU, there is no international network specifically dedicated to cooperation in e-commerce enforcement. However, the International Consumer Protection and Enforcement Network (ICPEN)[347], has recently taken steps to formalise international cooperation in enforcing of trading regulations.

11.43. ICPEN's econsumer.gov project[348] was unveiled in 2001 in response to the challenges of multinational internet fraud, and to enhance consumer protection and consumer confidence in e-commerce. It is a joint effort by 21 countries, whose objective is to gather and share cross-border e-commerce complaints from consumers. The project has a public website which provides general information about consumer protection in countries belonging to ICPEN, contact information for consumer protection authorities in those countries, and an online complaint form. Complaints filed by consumers are maintained on the Consumer Sentinel database operated by the FTC.

11.44. ICPEN also conducts annual international 'Web Sweep Days', where officials from across the network work in a coordinated fashion to assess and address a particular online issue – but again these have tended to focus on scams rather than on compliance with consumer protection regulation.

11.45. As well as this multilateral network, there are some international bilateral Memoranda of Understanding (MoUs) which exist between consumer bodies which enable the sharing of information and best practice. Examples involving the UK include:

- Memoranda of understanding on cross-border scams were signed by the OFT with the US Federal Trade Commission and the Canadian Competition Bureau in 2000 and 2003 respectively.
- The OFT, the Information Commissioner's Office and the FTC have signed a memorandum of understanding covering mutual enforcement of spam regulations; exchange of information and best practice including on technical remedies; cooperation on awareness-raising activities; and government-industry collaboration.
- Memoranda of understanding on cross-border cooperation were signed by the OFT with the Australian Competition and Consumer Commission and The Commerce Commission in New Zealand in 2003. These defined the scope of co-operation between the participant organisations and established a framework to share information, cooperate and coordinate enforcement activities in a more effective way than would otherwise be attained through independent action.

[347] ICPEN was launched in 1992 as a major inter-governmental initiative dealing with consumer fraud and infringements of trading regulations. ICPEN has 33 national members, as well as the OECD and the European Commission, all of whom agree to a Memorandum of Understanding. This Memorandum mandates them to: (a) establish and maintain an up-to-date list of relevant enforcement contacts; (b) attend annual conferences to exchange views and opinions on relevant topics; (c) mutually exchange information to enable participating organisations to build up a picture of each other's methods and legal and administrative arrangements; and (d) co-operate informally at an operating level in preventing marketing malpractices as they arise.

[348] See: www.econsumer.gov.

11.46. There have been some examples of international co-operation to address problems with traders selling online across borders (see Box 11.2 for an example). However, again, international co-operation has tended to focus more on security and other threats to internet users (including internet shoppers), rather than on assisting consumers who experience problems buying across borders from legitimate traders – for instance experiencing problems with delays or communications.

### Box 11.2: Case study – Cross-border enforcement

A business operating under the domain name www.myDV.co.uk was advertising electronic, computer and camera goods. The site appeared to give the impression that it was UK-based, from its name and also by stating on its home page that it was 'the UK's best source for digital video equipment'. The business was in fact based in America.

In 2005, Consumer Direct received 207 complaints about the company, including:

- Misleading consumers into believing that this was a UK-based business
- Various breaches of the DSRs, including selling items incompatible with UK specifications
- Failure to give consumers full product information
- Deceptive pricing (items quoted in sterling but consumers charged in US dollars)
- Failure to deliver the goods and, where goods were delivered, failure to offer cancellation rights and refunds
- Failure to provide a contact address.

Despite the high level of complaints, the absence of contact information on the website made it difficult to identify the whereabouts of the trader and hence the Home Authority TSS. Various 'footprints' (such as US dollar conversions and an American accent on the answer phone) suggested a trader based in the US, meaning the business would be outside the jurisdiction of the OFT. A blog set up by a disgruntled consumer identified the owner of the site and pointed to his being based in Massachusetts, USA. The Attorney General of Massachusetts was contacted and in December 2005 the trader was served with a Stipulated Order. The Order sought to bring an end to the poor behaviour of the trader and address the detriment suffered by consumers. By January 2006, myDV.co.uk had ceased trading.

## Conclusions

11.47. The scale of cross-border internet trade is relatively modest – both as a proportion of UK consumer spend and UK business sales. It accounts for approximately one-tenth of UK businesses' sales and one-tenth of UK shoppers' spend.

11.48. Internet shoppers' rights within the EU share a common framework, which includes requiring European e-tailers to provide a minimum seven working day cancellation period. This, along with measures such as the Consumer Protection Cooperation (CPC) Regulation, should help consumers to buy with confidence online from anywhere in the EU.

11.49. However, outside Europe, the protections for consumers are less well established. Some international agreements and networks exist, although these have tended to address general threats to internet users, such as spam and scams. These partnerships could provide a valuable basis on which to focus more attention on protecting consumers' rights when buying from online traders.

## Next steps

11.50. In earlier chapters we consider the importance of raising consumers' awareness of their rights. This should include raising awareness of what to look for to identify the location of a trader, as well as how to handle any problems that arise when buying from abroad. We will also explore with enforcement partners how to improve international co-operation in addressing problems arising from cross-border shopping.

# 12 CHANGES: LOOKING TO THE FUTURE

## Summary

A consistent theme throughout our research was how rapidly the internet environment is changing as a retail channel for businesses and consumers. Internet shopping is an exceptionally dynamic area, with important policy, regulatory, technical and market developments on an almost daily basis.

We have found many regulatory and policy developments of which consumer protection authorities, businesses and consumers need to be aware. Future developments which could have significant impacts include the outcomes of the EC review to harmonise and modernise the raft of consumer protection regulations, including those for distance selling. The Consumer Protection from Unfair Trading Regulations will introduce from 2008 principle-based regulation for B2C practices and impose a general duty not to trade unfairly. This could have major ramifications for consumer protection generally but also some specific implications for online trading.

But the internet and technology are also evolving at a dizzying pace with predictions emerging as rapidly as the technology changes. Possible future developments that could impact on consumers and businesses include advancements in search technologies that may empower users, improvements to security to counter ever-changing threats, and convergence of platforms (such as mobile commerce). The evolution of targeted advertising, intelligent machines ordering products on their owners' behalf, and the ongoing growth of virtual worlds also potentially present consumer protection issues.

However internet shopping evolves in the future, it seems clear that authorities charged with protecting consumers need to keep up and look ahead of the curve to new challenges.

## Next steps

We will now therefore consult key interested parties, to develop closer working relations and remedies to the issues we identify in our report. We will aim to put in place a forward-looking strategy for internet shopping which, in particular, will include:

- Working closely with Trading Standards Services, to identify how best to enhance and assist future enforcement of online shoppers' rights
- Developing a strategy of targeted, innovative campaigns to raise awareness of shoppers' rights, as well as other issues such as effective search, risks, redress and protections

We will announce the details of this strategy, and how we will be implementing it, by the end of the year.

## Introduction

12.1. A consistent theme throughout our discussions with stakeholders was that internet shopping is an exceptionally dynamic area, with important policy, regulatory, technical and market developments on an almost daily basis.

12.2. We consider briefly in this Chapter some of the key certain and possible developments in these areas and their potential implications for consumers, businesses and authorities charged with protecting consumers.

## Regulatory and policy developments

### Developments in the regulatory framework

12.3. We noted elsewhere some recent changes to the domestic regulatory framework, such as the Fraud Act 2006 in Chapters 3 and 10. In Chapter 11, we also addressed recent developments in the international regulatory framework, such as the Consumer Protection Co-operation Regulation.

12.4. Looking ahead, there are many further substantial regulatory changes at an international and domestic level that are likely to have implications for internet shopping in the future. These and other likely developments are outlined in Box 12.1.

### Box 12.1: Domestic and international regulatory developmentss

Developments include (this list is not exhaustive):

- The EC review of the **consumer acquis** (consisting of eight consumer protection Directives), is intended to harmonise and modernise the consumer protection framework. This includes the Distance Selling Directive 97/7/EC which is implemented into UK law by the DSRs.
- The **Consumer Protection from Unfair Trading Regulations** (CPR) implementing the Unfair Commercial Practices Directive will introduce from April 2008 principle-based regulation for business to consumer transactions. This will have an impact on existing UK law, and will result in the repeal of some B2C legislation. See below for further discussion.
- Proposed amendments to the **Rome I Convention** to convert the Convention into a Regulation and to modernise some of its rules on the law applicable to contractual situations. This is considered in Chapter 11. Debates and reports by the Council and the European Parliament were due at the time of writing.
- The second EC review of the **Electronic Commerce Directive** is due later this year with a possible revision of the Directive likely to follow in 2008.
- A **European Small Claims Procedure** which is expected to be finalised in June 2007 should, from 2009, make it easier to deal with cross-border cases for claims up to €2000 and be enforceable in all Member States.
- The EC proposed revision of the **'third package' for air travel**, which includes proposals to require air fares to include all non-optional taxes, charges and fees. The proposal has been the subject of negotiations by Member States and at the time of writing was due to be considered by the European Parliament in summer 2007.
- EC proposed **Directive on Payment Services** is aimed at establishing a legal framework which will make cross border payments as easy and secure as national payments within one Member State. At the time of writing, the European Parliament had approved the text from Council.

12.5. In the longer term, the outcomes of the EC's review of the main consumer protection regulations (the 'consumer acquis') could be particularly important to internet shopping, with important ramifications for some of the issues we have identified in our report, such as harmonisation of the cancellation period and whether or not online auctions should be exempt from distance selling legislation. We discussed these issues in Chapters 6 and 10.

12.6. Any changes to the DSRs resulting from the consumer acquis review will take place at some point over the next few years. However, the most immediate and significant regulatory development is likely to be the introduction of the Consumer Protection from Unfair Trading Regulations ('CPRs'), which we consider in more detail below.

### The Consumer Protection from Unfair Trading Regulations ('CPRs')

12.7. From April 2008, the CPRs will impose a general duty on businesses not to trade unfairly with consumers. The scope of this duty will be wide ranging – applying to all B2C commercial practices before, during and after a commercial transaction in relation to any goods or services. These Regulations,[349] which implement the Unfair Commercial Practices Directive (UCPD), will establish:

- a general prohibition of unfair commercial practices
- prohibitions of misleading and aggressive practices
- 31 specific practices which are prohibited in all circumstances

12.8. The Regulations will apply whichever retail channel a business uses – the High Street, mail order, telephone sales or the internet. However, some aspects of the Regulations could have particular relevance to internet retailers. For instance:

- the prohibition on misleading omissions, which could be particularly relevant to our findings on unclear information (Chapter 9)
- the requirement for retailers to provide specific information to consumers who place orders directly on their website ('Invitation to Purchase')
- some other prohibited practices, such as presenting existing legal rights (for instance, the cancellation rights under the DSR) as though they are a unique selling point offered by the retailer

### Box 12.2: Possible implications of the Consumer Protection from Unfair Trading Regulations ('CPRs') for internet shopping

**Misleading omissions**

Retailers who offer goods for sale to consumers on the internet will be breaching the regulations if they omit or hide material information,[350] or provide it in an unclear, unintelligible or ambiguous manner; or provide it at a later stage than the consumer needs to take an informed decision. Depending on the context, this might apply, for example if sites do not provide timely information about additional compulsory charges, or provide it in a page which can only be reached through a difficult to find hyperlink, or provide it after the consumer has indicated commitment to purchase the product.

[349] In May 2007, OFT/DTI issued a consultation document on draft illustrative guidance on the Consumer Protection from Unfair Trading Regulations (CPRs). See: www.oft.gov.uk/shared_oft/reports/consumer_protection/oft931con.pdf The comments here are not intended to provide detailed guidance but to indicate possible areas where the Regulations may have an impact on internet shopping.

[350] Material information in this context is information that the average consumer needs, in the context, to make informed decisions. It includes any information required by European derived (EC) law, such as the Package Travel, Package Holidays and Package Tours Regulations (SI 1992/3288) and the DSRs. What information is required will depend on the circumstances, for example what the product concerned is, and where and how it is offered for sale. This may range from a very small amount of information for simple products, to more information for complex products.

### Invitations to purchase

Commercial websites that let consumers place orders will need to meet the 'Invitation to Purchase' information requirements of the Regulations.[351] Normally, unless it is apparent to buyers from the context, traders will need to provide information on: the main characteristics of the product, the trader's geographical address and identity, the price inclusive of taxes, all additional freight, postal or delivery charges[352], arrangements for payment, delivery, performance, complaint-handling policy (if different from consumers' reasonable expectations), the existence of cancellation rights, and other information requirements of Community law.

In the context of internet shopping, the information requirements of Community Law would include those imposed under the DSRs, the ECRs and, for certain travel sites, the Package Travel Regulations.

A page or pages on a website with a price where consumers can place an order will normally be an invitation to purchase within the Regulations.

### Prohibited practices

Further, the Regulations provide a list of commercial practices which are always prohibited. A number of these will be potentially relevant to internet shopping sites, for example:

- Claiming to be a signatory to a code of conduct when the trader is not
- Displaying a trust mark, quality mark or equivalent without having obtained the necessary authorisation
- Claiming that a code of conduct has an endorsement from a public or other body which it does not have
- Presenting rights given to consumers in law as a distinctive feature of the trader's offer (for example, indicating that cancellation rights which must be given under the DSRs are a unique selling point of that trader)
- Using editorial content to promote a product where the trader has paid for the promotion without making that clear (advertorials)
- Falsely claiming or creating the impression that the trader is not acting for business purposes or falsely representing himself as a consumer.

## Developments in the enforcement framework

12.9. The regulatory changes described in the previous section will, of course, impact on the role and work of enforcers. In addition, however, there are ongoing developments in the domestic enforcement framework itself.

12.10. For example, in Chapter 8, we noted how the recent Gowers Review[353] had implications for LATSS in terms of strengthening the enforcement of intellectual property rights, whether through clamping down on piracy or trade in counterfeit goods.

[351] This is a different concept from an 'invitation to treat' in UK contract law. An invitation to purchase has the following elements: (a) it is a commercial communication; and (b) it indicates characteristics of the product concerned and the price, in a way appropriate to the communication medium used; and (c) it thereby enables the consumer to make a purchase.

[352] If these cannot reasonably be calculated in advance, details of how they will be calculated. If this is not possible, the fact that additional charges may be payable.

[353] Gowers (2006).

12.11. Likewise, the Rogers Review in March 2007 proposed national enforcement priorities for local authority regulatory services (Trading Standards and Environmental Health),[354] with six priorities of which one, the fair trading priority, was targeted at scams, rogue traders and IP crime. The recommendations from the Rogers review were accepted in full on publication of the Report.

12.12. In particular, recent developments include the drive towards better prioritisation and improved cross boundary, regional and national working between TSS, and between the TSS and the OFT (see Chapter 8). Of crucial significance is the Regulatory Enforcement and Sanctions Bill[355] to implement the:

- recommendations of the Macrory Review of Regulatory Justice,[356] for sanctions to be more flexible and risk-based
- plans for the Local Better Regulation Office (LBRO), to encourage consistent and coordinated risk-based enforcement and inspection at local authority level.

12.13. These developments are outlined in Box 12.3.

### Box 12.3: Developments in the enforcement framework

**Making sanctions more effective**

Sanctions are an important feature of any enforcement regime. They should ensure that businesses that do not comply with their regulatory obligations are punished.

The finding of the Macrory review suggested that many regulators are heavily reliant on criminal prosecution, as the main sanction tool for various misdemeanours. The findings of the review went on to suggest that criminal prosecution may not be, in all circumstances, the most appropriate sanction to deal with non compliance and ensure a change in behaviour. What was missing was the availability of other more flexible and risk based tools which may result in achieving better regulatory outcomes.

The review recommended that Government consider a different approach to regulatory justice by, amongst other things:

- Examining the way in which it formulates criminal offences relating to regulatory non compliance
- Introducing schemes of Fixed and Variable Monetary Administrative Penalties, available to those regulators who are Hampton compliant, with an appeal to an independent tribunal instead of the criminal courts

Introducing alternative sentencing options in the criminal courts for cases related to regulatory non-compliance.

[354] National enforcement priorities for local authority regulatory services.

[355] Further information can be found at: www.cabinetoffice.gov.uk/regulation/reform/hampton/latest.asp.

[356] Macrory (2006).

### Local Better Regulation Office (LBRO)

In the 2006 Pre-Budget Report, the Better Regulation Executive (BRE) was tasked with setting up the Local Better Regulation Office (LBRO) to encourage the implementation of a consistent and coordinated risk-based approach to enforcement and inspection at local authority level.

The overall objective of the LBRO will be to secure more effective and less burdensome approaches to the way in which regulations are enforced by local authorities. Its remit will initially extend to TSS and environmental health regulatory services, including alcohol licensing. It is possible that LBRO's scope will in the future be increased to include other services.

LBRO's five key functions (based on the May 2007 consultation on the draft Regulatory Enforcement and Sanctions Bill) are:

- improving the coordination and consistency of regulatory functions and enforcement through the Primary Authority Principle, resolving disputes when they arise;
- issuing guidance to local authorities in respect of regulatory services;
- reviewing and revising a list of national priorities for local authority regulatory services;
- providing advice to Government on enforcement and regulatory issues associated with local government; and
- encouraging best practice, and innovative approaches to the provision of local authority regulatory services, including through the use of its programme budget.

The LBRO was established as a Cabinet Office owned company limited by guarantee on 4 May 2007. This company will be dissolved and replaced by a non-departmental public body with identical aims and objectives when the Regulatory Enforcement and Sanctions Bill is enacted.

## Market developments

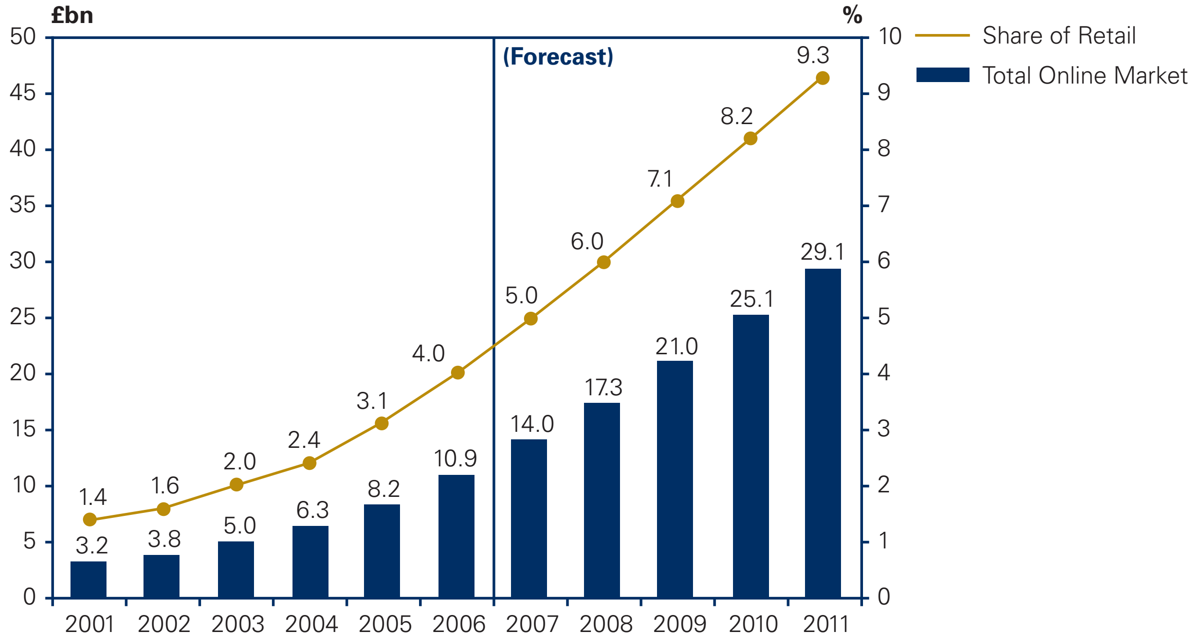
12.14. The regulatory and enforcement developments described above are all taking place against the background of growth in the internet as a retail channel and rapid market and technological changes. The sheer pace of evolution in internet shopping presents significant and unique challenges to consumers, businesses and enforcers.

### Market forecasts

12.15. Predictions suggest that the market for internet shopping will continue to grow rapidly, although there are major variations in the size and nature of these forecasts. For example, Verdict forecast retail sales to nearly triple from £10.9bn in 2006 to £29.1bn by 2011. This means that online shopping would more than double its share of overall retail spending, from 4.0 per cent to 9.3 per cent (see Chart 12.1).

12.16. Taking this even further, research from the Centre for Economics and Business Research (CEBR) predicts that online sales could comprise 40 per cent of all retail sales by 2020, at a value of equivalent to £162bn

**Chart 12.1: Forecast of online retail spending to 2011**



Source: Verdict (2007b)

12.17. When we surveyed online retailers who had sold online for at least a year, we found that most of them were optimistic about prospects for growth. Asked to compare share of sales via the internet this year with last, 22 per cent claimed it was a lot higher and 29 per cent a little higher. Asked for their projections for next year, 35 per cent expect internet sales to be a lot higher and 41 per cent a little higher.

## Technological developments

12.18. This growth in internet shopping will take place within the context of rapid developments in the internet more generally. There continues to be a lot of interest in how the internet is developing and the implications for consumers – for instance, at events such as the US Federal Trade Commission's hearings in November 2006 on 'Protecting Consumers in the Next Tech-ade'.[357] Predictions of what the future holds for the internet vary significantly, but our analysis of recent literature in this area points to agreement on some underlying trends:[358]

- It is widely felt that there will be increasing take up of the internet, both generally and across social groups. This could enable more consumers to benefit from convenience, choice and lower prices, but it may also expose less aware and more vulnerable consumers to threats and shopping problems

- The internet is likely to be faster, 'always on', and accessed through a wider range of devices, such as mobile phones and digital TVs. Convergence of platforms (e.g. media centres, TV-based internet access, m-commerce), will offer increasingly varied ways to buy online, but may blur regulatory boundaries and require updates in regulations.

[357] The FTC's public hearings on Protecting Consumers in the Next Tech-ade took place in November 2006. The hearing panels examined the key technological and business developments that will shape consumers' core experiences in the coming ten years. See: www.ftc.gov/techade

[358] As well as the FTC Next Tech Ade Conference, recent examples include the 2006 OECD Workshop on the 'Future of the Internet' (see: www.oecd.org/dataoecd/26/36/37422724.pdf?bcsi_scan_A2018E0826464712=1), and Pew (2006).

12.19. Beyond these areas, however, clear consensus is hard to find amidst much speculation. Many of the emerging trends which are identified by commentators could, if they continue to develop, have a significant impact on the future of businesses and consumers transacting on the internet. We briefly discuss some examples of others' predictions in Box 12.4:

- advancements in search technologies that may empower users
- the evolution of targeted and mobile advertising
- intelligent machines ordering products on their owners' behalf
- the ongoing growth of virtual worlds

### Box 12.4: Some forecasts of technological developments

#### Reduced distance between buyers, sellers and goods

The conceptual distance between buyers, sellers and goods that exists online may close in the near future. As bandwidth increases, a large amount of online content could shift from text to video and interactive media. Consumers may soon be able to watch products in action, and interact with them. With developments such as 'haptic' technology, they may even be able to 'feel' them. As well as getting closer to products, consumers may also be able to get closer to sellers. Communication could migrate from email to video conferencing.

#### Semantic web

The semantic web is characterised by the tagging and categorisation of words and websites with common search terms. This facilitates the interpretation of websites by computers as well as people and is already under way. Semantic search could cut through the vast amounts of information on the web by searching for the meaning of a phrase, rather than just the actual words entered. For internet shoppers, these searches could make the process of finding the right product quicker, easier, more accurate and less frustrating.

#### Behavioural marketing and automation

Some advertisers suggest that by understanding their customers better, they can target adverts that will be relevant to consumers. The internet might provide the window into consumers' lives that advertisers seek, as the websites they view, the products they browse, and the decisions they make can be logged and analysed. Some commentators have suggested that this will lead to more focussed, relevant and informative advertising for consumers. Others think that consumers could feel uneasy about the extent to which their actions are being monitored.

One organisation we spoke to suggested that 'nagware' may remind consumers to make purchases. While this may inform consumers and assist competition, it could affect confidence by raising fears about information access and use. Likewise, 'machine-based ordering' (such as fridges ordering stock, TVs downloading programmes) may help consumers, but raise new issues over contract formation and redress.

#### Mobility, locational information and advertising

Mobile access to the internet combined with GPS technology could blur the boundaries between online and offline shopping. Consumers who have been searching for a particular product online might receive adverts and directions on a mobile device as they approach a high street store that has the product. Furthermore, consumers in a retail store might be able to access price comparison and product information websites, as well as receive adverts from nearby stores who may have a better deal.

**Web 2.0 and user generated content**

Web 2.0 refers to the rapid growth of collaborative, user generated content on the internet. Wikipedia and Flickr are early examples of this trend. Consumers are increasingly the creators of content, much of which affects existing e-commerce models from user reviews of products and services in forums to blogs (web logs) that often discuss brands and trends. This could allow individuals to express themselves more confidently as consumers.

**Metaverse: virtual worlds with real markets**

Virtual worlds contain real markets, and are expanding rapidly. One of the most high profile of these, Second Life, is growing at a rate of 40 per cent per month. Users can buy and sell objects they design and rent out their 'land'. Furthermore, established firms as diverse as Toyota, Nissan, Nike, Reebok, Reuters and Channel 4 have a growing commercial presence in the 'metaverse'. One economist Edward Castronova has valued the economy of the metaverse at USD4.8bn.[359] Other estimates are as high as USD7.3bn.[360] To date, there has been little attention paid to the potential consumer protection issues that might be raised by these new forms of retailing.

## Conclusions

12.20. As well as addressing the issues we identified, we need to look ahead to new developments. The backdrop to internet shopping is changing at a dizzying pace, with developments such as mobile phone commerce, targeted advertising, digital delivery and Web 2.0. Furthermore, the law and its enforcement are evolving, with possible changes from a review by the European Commission; the introduction of the Consumer Protection Co-operation Regime and the Consumer Protection from Unfair Trading Regulations; as well as the establishment of the Local Better Regulation Office.

12.21. However internet shopping evolves in the future, it seems clear that authorities charged with protecting consumers need to keep up and look ahead of the curve to new challenges.

## Next steps

12.22. We will now therefore consult key interested parties, to develop closer working relations and remedies to the issues we identify in our report. We will aim to put in place a forward-looking strategy for internet shopping which, in particular, will include:

- Working closely with Trading Standards Services, to identify how best to enhance and assist future enforcement of online shoppers' rights
- Developing a strategy of targeted, innovative campaigns to raise awareness of shoppers' rights, as well as other issues such as effective search, risks, redress and protections

12.23. We will announce the details of this strategy, and how we will be implementing it, by the end of the year.

[359] See:observer.guardian.co.uk/review/story/0,,1933933,00.html.

[360] See: hyamaguti.cocolog-nifty.com/virtualworlds/2005/04/virtual_world_g.html.

Published by the Office of Fair Trading
Printed in the UK on paper comprising 75% post-consumer waste and 25% ECF pulp
Product code OFT921
Edition 06/07 Printed: 06/07/400