

protecting consumers online

a strategy for the UK

December 2010

OFT1252

© **Crown copyright 2010**

You may reuse this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit www.nationalarchives.gov.uk/doc/open-government-licence/ or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk

Any enquiries regarding this publication should be sent to us at: Marketing, Office of Fair Trading, Fleetbank House, 2-6 Salisbury Square, London EC4Y 8JX, or email: marketing@oft.gsi.gov.uk

This publication is also available from our website at: www.oft.gov.uk.

CONTENTS

<i>Chapter/Annexe</i>	<i>Page</i>
1 Foreword	4
2 Executive Summary	6
3 e-consumer protection – the ambition	9
4 Evidence review	14
5 Actions – Developing more effective enforcement	40
6 Actions – Promoting business compliance	50
7 Actions – Empowering consumers	56
8 Next steps	64
A Responses to consultation	80
B Levels of e-consumer Internet Enforcement	81
C Glossary of terms	82

1 FOREWORD

A quarter of a century ago, the first '.co.uk' name was registered. By 2009, the internet had contributed an estimated £100 billion to the UK economy. In the same period, consumers collectively spent around £50 billion online on goods and travel.¹ Sometimes referred to as the fifth utility, the internet has become an established and essential tool in many people's lives.

The Office of Fair Trading (OFT) works to help safeguard the economic interest of consumers who use the internet by taking enforcement action where necessary, but also by influencing businesses, coordinating action across the local authority Trading Standards Service (TSS) network, liaising with enforcers and policy makers across the EU and globally, and working with consumer bodies to educate and inform consumers. In a world with fewer borders, our response to consumer protection at a national and international level must adapt and reflect the impact of online technologies and habits.

The OFT was charged by government in the July 2009 Consumer White Paper to develop a UK strategy for protecting consumers online. The strategy outlined in the following pages proposes a number of recommendations to strengthen e-consumer protection in the UK, and has been developed in consultation with TSS, industry, consumer groups and the general public. The recommendations are a call to action, not only for the OFT but also for consumers, consumer groups, industry, enforcers and central government.

Recent announcements by the Secretary of State for the Department for Business Innovation and Skills (BIS),² driven by the need to reduce public spending and rationalise the delivery of public services, suggest changes to the

¹ 'The Connected Kingdom', The Boston Consulting Group, October 2010
www.bcg.com/documents/file62983.pdf

² The Secretary of State has said he is 'minded to shift almost all relevant Central Government funding for consumer bodies towards [Citizens Advice and Trading Standards]... Trading Standards will be given responsibility for enforcement of almost all consumer law. ... national and regional threats will now increasingly also be addressed through one or more dedicated, expert teams, within Trading Standards with work coordinated nationally for this purpose.'

consumer protection landscape. While the recommendations for protecting consumers outlined in this strategy will need to be revisited once the eventual shape of the consumer landscape is clear, many will remain valid irrespective of who is responsible for consumer issues.

In reading the strategy, where we refer to the OFT, this is in the context of the present structure of the consumer regime. It should therefore be understood as also referring to any relevant organisation, be it a particular TSS or any body or bodies that will have enforcement, coordination or other relevant responsibilities in future at national, regional or local level. Other references to existing organisations should also be translated in a similar fashion.

Our aim, together with other groups across industry and government is to increase UK consumers' confidence in the internet even further and to support the growth of this very dynamic sector of the economy. We hope that as a result, consumers will enjoy another 25 years of innovation and significant benefits from e-commerce.

Philip Collins
Chairman of the OFT

2 EXECUTIVE SUMMARY

- 2.1 The UK has a vibrant internet economy, with strong online participation, high levels of trust and comparatively substantial online spend.³ Fraud associated with the use of credit cards online is declining.⁴ Business compliance is increasing. On the whole, consumers feel they have the right level of protection, and trust public authorities (see Diagram 1, page 10).
- 2.2 This strategy builds on the inherent strengths of the UK internet economy, promoting best practice and addressing barriers to consumer protection online. With average savings per household of £560 per year from shopping and paying bills online,⁵ and around 40 per cent of the UK population not transacting online (rising to 56 per cent of social groups DE, based on 318 responses)⁶ consumers, particularly the most vulnerable, could be missing out on significant benefits.
- 2.3 The need for a more coherent approach to protecting consumers online arose in response to concerns identified by the government in the July 2009 Consumer White Paper. The objective of this strategy is to enable the OFT, TSS and other agencies to work together more effectively.

³ High levels of trust – see Diagram 1, page 10; High levels of participation – see 'Individuals who ordered or purchased goods or services on the Internet, as a percentage of adults', Source: OECD ICT Database. In 2008 at 57 per cent UK individuals had the third highest participation rate in the OECD.

⁴ UK Cards Association, 2010, 'Fraud the Facts 2010', www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

⁵ Source: The Economic Case for Digital Inclusion, October 2009, www.parliamentandinternet.org.uk/uploads/Final_report.pdf

⁶ Social classes DE, from Attitudes to Online Markets (OFT1253), FDS, August 2010, www.of.gov.uk/shared_of/consultations/eprotection/oft1253

- 2.4 The strategy explicitly focuses on protecting consumers from economic harm and raising consumer awareness of their rights when transacting online. It does not look at issues of personal safety and security or national security.⁷
- 2.5 A strategy consultation was published in July 2010 and received 45 responses. During the consultation, a number of workshops were held with a range of industry groups, consumer bodies, businesses and non-profit organisations. The consultation was publicised in a number of online blogs, magazines and emails.
- 2.6 Responses to the consultation and a detailed evidence review have highlighted the fragmented nature of enforcement, the range of internet enforcement capability across the 198 TSS, the low (but increasing) levels of business compliance with consumer protection legislation, and the low levels of consumer awareness of their rights.
- 2.7 Some key aspects of consumer protection will need to improve if the UK is to maintain or improve its current level of protection for consumers: more effective enforcement, greater business compliance and better consumer understanding of their rights.
- 2.8 Specifically, for more effective enforcement we need to:
- improve data-sharing and intelligence between the OFT and TSS, across the UK and nationally
 - increase coordination of enforcement (where this is possible without compromising sensitive investigations)
 - develop internet enforcement capability within the OFT and TSS, and across the UK.

⁷ There are many organisations whose remit covers personal safety and security, such as CeOPs, Get Safe On Line, OCSIA, Race Online 2012 etc. amongst others who are already looking at these issues.

2.9 Increasing business compliance can be promoted through:

- better guidance for businesses on how to comply with consumer protection regulations and by making it easier for businesses to find relevant guidance materials
- working jointly with business to design-in compliance and to share information for the purposes of intelligence and horizon scanning.

2.10 We can help empower consumers by:

- educating consumers about their online rights and working with consumer bodies to ensure consistent messages
- working on initiatives that improve the transparency of the transactions, and the security of payment mechanisms
- improving the access and quality of consumer redress, and consumer learning (for example, consumer feedback and rating sites).

2.11 The great strength of the internet is in its ability to innovate rapidly, and to enable audiences to interact, exchanging goods and ideas worldwide. While this can create challenges for enforcers and consumers alike, it can also bring substantial benefits. The Boston Consulting Group has calculated that the UK's internet economy represented 7.2 per cent of GDP in 2009.⁸

2.12 We believe that the recommendations outlined in this strategy will improve consumer protection in the UK and help support sustainable increased growth.

⁸ 'The Connected Kingdom', The Boston Consulting Group, October 2010
www.bcg.com/documents/file62983.pdf

3 E-CONSUMER PROTECTION – THE AMBITION

- 3.1 Within the UK, consumer confidence in the internet is relatively high compared to other European countries (see Diagram 1), scoring in the top four countries on all elements of trust measured. However a survey conducted by FDS International in January 2010 indicates that 19 per cent of UK internet users are not transacting online, and approximately one third of these people are not doing so due to worries about the security of their personal and financial details.⁹
- 3.2 There are other areas of concern: two-thirds of internet users are worried about others accessing their personal details on the internet. One-quarter of internet users engaging in e-commerce are 'much more worried' about losing out to or being conned by companies when they buy online compared to when they buy offline, and 37 per cent are a 'little more worried'.¹⁰ These sorts of concerns can easily translate into lower levels of internet usage in the long term than consumers and businesses consider ideal.
- 3.3 Households are missing out on potential savings of an estimated £560 per year per household by not shopping or paying bills online. The total benefits to the UK of getting everyone online are estimated to be in excess of £22bn.¹¹ In 2007, the OFT calculated that this represented between £175m and £350m in missed savings for consumers every year¹² (for example, Which? list typical online savings on a range of household goods, which range from 14 per cent on books to 29 per cent for CDs/Plasma TVs¹³).

⁹ Attitudes to Online Markets (OFT1253), FDS, August 2010, www.offt.gov.uk/shared_offt/consultations/eprotection/offt1253

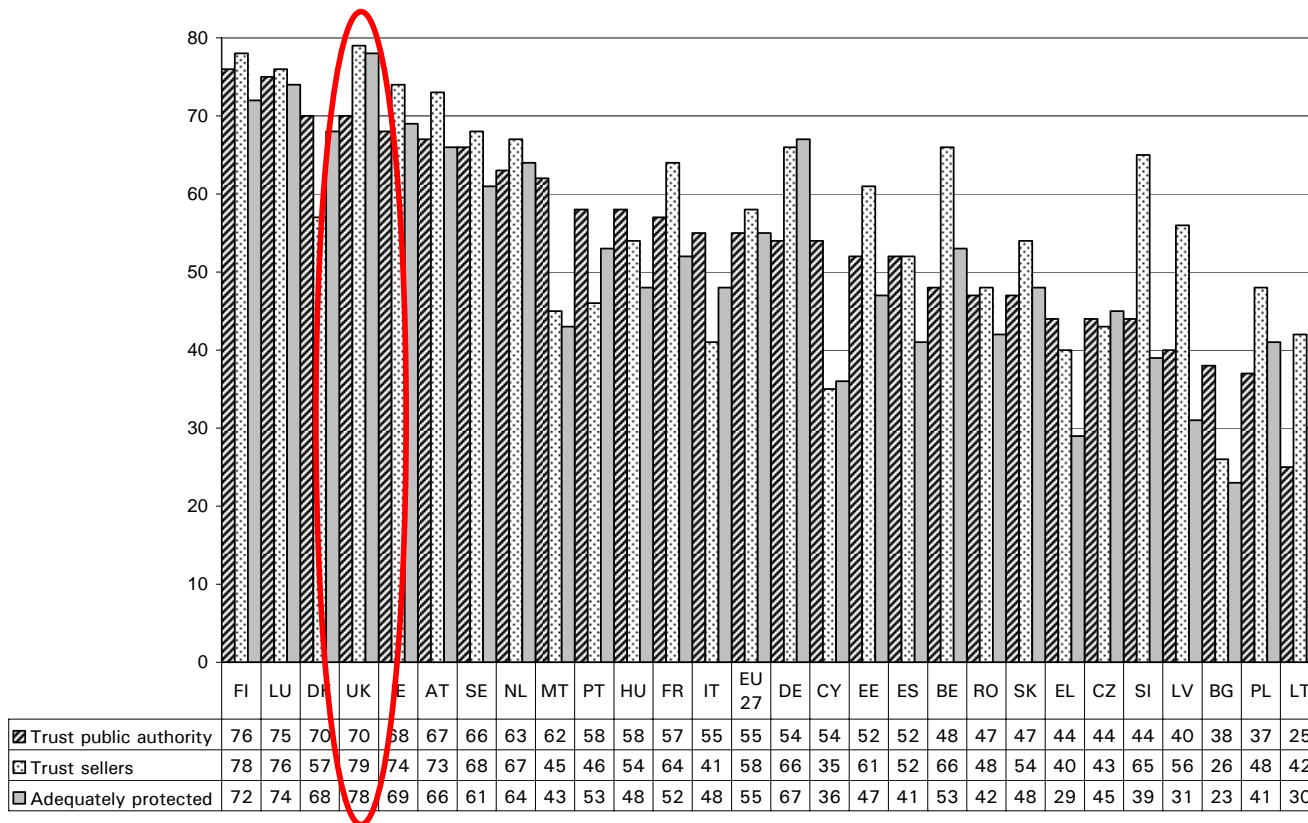
¹⁰ ibid

¹¹ Source: The Economic Case for Digital Inclusion, October 2009

¹² 'Internet users who are too worried to buy online could be missing savings of £175m to £350m each year.', from 'Internet Shopping, An OFT Market Study, 2007', www.offt.gov.uk/shared_offt/reports/consumer_protection/offt921.pdf

¹³ 'Internet Shopping, An OFT Market Study, 2007', ibid

Diagram 1 Consumer feelings about adequate protection and trust relating to internet transactions within the EU



Source: The Consumer Markets Scoreboard 3rd edition, European Commission, 2010, ec.europa.eu/consumers/strategy/docs/3rd_edition_scoreboard_en.pdf

- 3.4 These online savings generally arise as a result of the increased competition due to market transparency, the elimination of intermediaries and the impact of operational savings.
- 3.5 This loss of potential savings is of particular concern for low income households (LIH, those earning less than 60 per cent of the median equivalised household income), which make up approximately 20 per cent of all households.¹⁴ LIH face a variety of disadvantages in terms of price (higher prices for prepay, risk-based pricing etc), quality and accessibility. The internet, both access to it, and transacting on it can compensate for these disadvantages. It is one of a set of potential enablers for LIH, alongside access to bank-accounts and car ownership.
- 3.6 While use of the internet may compensate for the disadvantages LIH face, the internet has the potential to reinforce price differentials. The amount of publically available information, coupled with a user's purchase history and geography could allow firms to target pricing, negatively affecting LIH. However our recent study on Online Targeted Advertising and Prices¹⁵ found no evidence of this by firms.
- 3.7 Amongst people who use the internet for personal use those from social classes DE are less likely to partake in e-commerce than those from classes AB (77 per cent vs. 90 per cent, based on 180 and 219 responses respectively). Social classes DE also use the internet to buy goods and services less frequently than classes AB (11 per cent of users from classes DE use the internet to buy goods and services at

¹⁴ Research commissioned by the OFT 'Markets and Households on Low Income', J Green (Europe Economics), P Kenway (New Policy Institute), June 2010, www.offt.gov.uk/shared_offt/research/OFT1268.pdf

¹⁵ Online Targeting of Advertising and Prices, A market study, May 2010 www.offt.gov.uk/shared_offt/business_leaflets/659703/OFT1231.pdf

least once a week, this more than doubles to 24 per cent of classes AB, these figures are based on 234 and 263 responses).¹⁶

- 3.8 Without effective use of (and trust in) the internet by LIH, competition in other markets (such as energy markets, telecoms or financial services) may be adversely affected. The internet in general and price comparison websites in particular create much greater price transparency. The internet facilitates competition, and may increase the range of offerings that are provided to LIH, who in general are not as well served as other segments of the population.
- 3.9 The aim of the strategy for protecting consumers online is to improve the working of online markets, and ensure that the UK is one of the global leaders in online enforcement. We wish to ensure consumers, where they so wish, can take advantage of the range and prices of products and services offered online.
- 3.10 Our ambition for the UK is a strong, consistent internet enforcement capability driven by excellent, high-quality intelligence. We see this being accompanied by high levels of business understanding of and compliance with Consumer Protection (Distance Selling) Regulations (DSRs), Consumer Protection Regulations and other consumer protection law, and strong co-operation between OFT, TSS and businesses. Aware, well informed consumers, who understand the nature of the internet and their online rights would reinforce this high-level of compliance.
- 3.11 This ambition translates into three clear objectives:
- to protect the economic interests of consumers online, and reduce the economic harm caused to consumers

¹⁶ Attitudes to Online Markets (OFT1253), OFT, July 2010, www.of.gov.uk/shared_of/consultations/eprotection/oft1253

- to increase the UK's enforcement capability to deal with e-consumer protection issues, and facilitate a coordinated approach to e-consumer protection
- to increase business awareness and compliance with DSRs, Consumer Protection Regulations and other consumer legislation.

3.12 In terms of understanding how well we are doing in achieving this ambition, we would like to monitor changes over time of the following elements:

- **internet effectiveness:**
 - **enforcement capability** - UK's e-protection enforcement capability, capacity and its effectiveness
 - **intelligence and coordination:** the take-up of standardised intelligence systems, the number of information sharing agreements, time taken to ascertain enforcement responsibilities
- **business compliance:** the creation of a web site containing guidance for businesses and consumers on DSRs, levels of compliance with DSRs and other consumer protection regulations as measured by web sweeps
- **consumers confidence in online markets:** awareness of their online rights, where to go for assistance, consumer attitudes to enforcement, redress and confidence.

4 EVIDENCE REVIEW

- 4.1 The UK has a successful internet economy, with strong online participation, high levels of trust and comparatively substantial online spend against other European countries. Consumers on the whole feel they have the right level of protection, and trust public authorities.¹⁷
- 4.2 Nonetheless, following public consultations, workshops with consumer bodies, industry and enforcers, and a review of available evidence, there are three broad areas where the UK could build still further on its successes:
- **improving enforcement:** coordination and intelligence sharing could be improved, there is lack of clarity over remits, and internet enforcement capability needs to be developed across the TSS and OFT
 - **promoting compliance:** businesses are not clear where to go to for advice, guidance could be improved, and enforcement agencies and businesses could work together to greater effect
 - **empowering consumers:** consumers don't always know their online rights or where to go to for help, the consumer landscape is fragmented with consumer organisations conveying a variety of messages regarding internet safety, and access for consumers to redress and learning can often be limited.

¹⁷ The Consumer Markets Scoreboard 3rd edition, European Commission, 2010, ec.europa.eu/consumers/strategy/docs/3rd_edition_scoreboard_en.pdf; see also for High levels of trust – Diagram 1, page 10; High levels of participation – see 'Individuals who ordered or purchased goods or services on the Internet, as a percentage of adults', Source: OECD ICT Database. In 2008 at 57 per cent UK individuals had the third highest participation rate in the OECD. High spend www.retailresearch.org/onlinetailing.php, with the UK having 9.7 per cent of retail trade conducted online, this is the highest in Europe

Enforcement

Leverage Intelligence

- 4.3 There is widespread agreement about the need to share consumer complaints data and internet intelligence both nationally and internationally, which came out clearly in both responses to the consultation and workshops held with other enforcement bodies. There was less agreement however as to how this should be achieved, and the chosen method or system that should be used.
- 4.4 Currently TSS and the OFT use complaints information from Consumer Direct (CD) and intelligence held on the Intelligence Management Database (IMD) (used by all Regional Intelligence Officers across Great Britain, and currently being rolled out to TSS) and other regional or national systems. Other sources include consumer organisations, such as Citizens' Advice and Which?, the Interactive Media in Retail Group (IMRG), SafeBuy, National Fraud Intelligence Bureau (NFIB) and other organisations from the UK and overseas.
- 4.5 More widely, Regional Intelligence Officers (RIOs) and case investigators develop intelligence during investigations, using intelligence software to pull together publically available information on the internet, undertaking covert intelligence gathering and sharing intelligence with other enforcers.
- 4.6 There were originally 11 dedicated RIO posts across Great Britain. These were established following seed funding from BIS, which came to an end in March 2009. Currently there are nine dedicated posts. Not all regions have decided to continue funding a specific RIO post and are trying to address the information and intelligence gap in alternative ways. A reduction in the effectiveness of the intelligence network will ultimately impact negatively on consumer enforcement effectiveness, as infringements remain undiscovered, cases lack the evidence required to pursue them and prioritisation is weakened without effective information to take decisions.

- 4.7 Recent work by the International Consumer Protection and Enforcement Network (ICPEN¹⁸) suggests that in terms of best practice, agencies should promote and encourage the use of a more systemised operation and use of intelligence by having dedicated human and capital assets, with the requisite mix of skills and competencies, appropriate technologies and the appropriate hardware and software. The RIO network, with its dedicated intelligence resources, addresses many of the points identified with the best practice model outlined above.
- 4.8 The OFT has shared data and intelligence with other enforcers outside the TSS network on an ad hoc basis, following procedures designed to ensure compliance with the Enterprise Act (2002) and other regulations including the Data Protection Act (1998). The OFT is looking at making this process more streamlined and automated, as well as seeking further legal advice on information sharing. Workshops with representatives from a range of enforcement agencies including TSS strongly supported the sharing of Consumer Direct data more widely.
- 4.9 Respondents however, felt that more needed to be done. Enforcement agencies could link up their databases more widely, and more use could be made of third party systems. An online reporting system, for example, could facilitate the capture of data which is not currently reported through either the NFIB or Consumer Direct.
- 4.10 The Association of Chief Police Officers (ACPO) in its e-crime strategy¹⁹ also touches on the issue of developing a clear national picture – 'Although forces can record and investigate e-Crime, the nature of e-Crime and the structure of existing recording frameworks make analysis at a national level difficult' and identifies one of the key issues, under-reporting by consumers and victims: 'Although the difficulties involved in gathering accurate data on e-Crime are widely

¹⁸ 'Final Report on Findings From Survey On ICPEN Intelligence Functions', April 2010

¹⁹ ACPO e-Crime Strategy, Version 1.0, 28 May 2009, www.acpo.police.uk/asp/policies/Data/Ecrime%20Strategy%20Website%20Version.pdf

acknowledged, ACPO is committed to developing more reliable and consistent measures of e-Crime... There are a number of barriers that will need to be overcome to accurately assess the level of e-Crime being committed on UK victims. One of the most significant challenges is under-reporting.'

- 4.11 In the Cabinet Office document *Cyber Security Strategy of the United Kingdom*,²⁰ two of the elements of the strategy are 'Gather intelligence on threat actors', and 'Improve knowledge and awareness'.

Build Enforcement Capability

- 4.12 A number of TSS Internet enforcement centres of expertise exist across the UK, which are well staffed and resourced, and are delivering highly effective internet enforcement. The UK's internet capability could be made efficient and effective by building on these existing centres.
- 4.13 A number of case examples for TSS internet enforcement are discussed below. These have been provided by the TSS themselves to help describe internet enforcement at a local authority level:

²⁰ Cyber Security Strategy of the United Kingdom, June 2009, www.cabinetoffice.gov.uk/media/216620/css0906.pdf

Case Example: Conwy TSS (Level 3)²¹

- 4.14 Conwy, a Unitary Authority in North Wales, is funded as a dedicated e-crime team in TSS by the Regulatory Services in Conwy. They are enforcement partners with North Wales Police and a number of authorities to the East and West (with one they have formal collaboration for enforcement purposes).
- 4.15 Conwy's e-crime team consists of two dedicated e-crime officers who investigate and enforce e-crime and also conduct computer forensic examinations. The team also has a Principal TSO who conducts computer forensic examinations. In addition to the internet investigations setup, Conwy has a computer forensic lab that is fully equipped to conduct forensic analysis on digital equipment.
- 4.16 Conwy has taken a number of cases, prosecuting traders selling fake football equipment, and online auction scams.²² On occasion Conwy has enforced outside of its authority when a Conwy consumer has been affected and the TSS which has responsibility for the area in which the suspect is based does not have the capability to investigate or enforce e-crime. Agreement from the relevant TSS has always been sought, and Conwy has offered them wider involvement in the investigation.

²¹ For definition of Levels of Enforcement see Annexe B

²² www.dailypost.co.uk/news/north-wales-news/2009/10/22/man-s-340-000-fakefootball-gear-scam-55578-24989528/
www.thefreelibrary.com/WALES%3A+Ex-council+man+jailed+for+eBay+clothes+fraud%3B+Scores+of+fake...-a0169484380
www.dailypost.co.uk/news/north-wales-news/2008/10/08/north-wales-man-sold-fake-guccis-on-ebay-55578-21988101/
www.dailypost.co.uk/news/north-wales-news/2008/06/18/fake-goods-trader-made-100-000-on-ebay-55578-21092223/

Case Example: Trading Standards North West (Level 1 to 2)

- 4.17 In Trading Standards North West (TSNW), five authorities have set up a covert Test Purchase facility, albeit at different levels of sophistication and with different equipment. Other authorities are interested in developing similar facilities as a result of the BIS funding. Each Local Authority (LA) funds their own activity.
- 4.18 In TSNW, each LA has a Local Intelligence Liaison Officer (LILO) who receives intelligence from the RIO who then disseminates it to the appropriate officers in their LA. Intelligence is fed upwards in the same manner. This operates independently from any e-Crime investigations but intelligence from them could and is fed into the process. Some officers will also feed intelligence into brand owners, specifically those that work to take websites down.

Case Example: Surrey County Council TSS (Level 1 to 2)

- 4.19 Surrey County Council Trading Standards is currently located in Leatherhead (moving to Reigate, 10 December 2010) and hosts Trading Standards South East and the Regional Fraud Unit (Scambusters).
- 4.20 Currently, there is no formal e-crime investigations unit. However, there are several TSOs who regularly carry out e-crime and related investigations. These are carried out using a stand-alone PC which complies with the ACPO good practice guide for Computer Based Electronic Evidence.²³ The officers also have access to a stand alone PC for accessing material during investigations which is not permitted when using Surrey County Council Trading Standards corporate PCs due to its inappropriate content etc.

²³ www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

- 4.21 The stand-alone set up is fully supported by the Trading Standards Applications Specialist who will be reviewing the current e-enforcement hardware/software provision after the service has moved to Reigate. It is envisaged that Surrey County Council Trading Standards will invest in additional kit (laptops) for carrying out E-Crime investigations and that there will be a shift away from traditional operating systems and configurations used to carry out such investigations.
- 4.22 There needs to be a fresh approach to how investigations are carried out (this includes the architecture of the equipment and tools used) and by whom (competency levels do vary).
- 4.23 Surrey County Council Trading Standards has a dedicated Intelligence Officer who is embedded in the service and acts as the conduit for interacting with other agencies (NFIB etc). Surrey County Council Trading Standards has, on one occasion, assisted another local authority with an electronic test purchase.
- 4.24 Surrey County Council Trading Standards has undertaken a number of successful prosecutions with regards to e-Enforcement investigations, including offences relating to selling and possession of counterfeit goods and offences under the Consumer Protection from Unfair Trading Regulations 2008 (CPRs).

Case Example: Carmarthenshire County Council (Level 3)

- 4.25 Carmarthenshire County Council is a unitary authority in South Wales. The Trading Standards service, which has limited resources available to it, evaluated digital crime as critical on the basis of risk for the purpose of consumer protection and economic prosperity. As such, in 2006 the service developed a digital enforcement strategy in order to target online and digital crime.

- 4.26 As part of the digital crime strategy, the service used Gowers Funding Grant²⁴ and proceeds of crime confiscations in order to fund the creation of a digital forensic facility capable of conducting forensic examination of digital equipment such as computers, mobile phones, iPods and any other equipment containing a memory. The facility further developed an internet investigations capability, with specialist stand-alone equipment, covert accounts, addresses and banking data.
- 4.27 The digital crime team consists of one dedicated forensic examiner who conducts computer forensic examinations, and one dedicated internet investigations officer who highlights and collates digital evidence for enforcement by five general Trading Standards staff. The team also has a Senior TSO who oversees the strategy and who also conducts computer forensic examinations.
- 4.28 Carmarthenshire Trading Standards Digital Crime Team are enforcement partners with Dyfed Powys Police and a number of organisations such as Scambusters, Federation Against Copywrite Theft (FACT), British Recorded Music Industry (BPI) and other local authorities. Once established with the Gowers Grant, the team, through use of ongoing proceeds of crime confiscations and court cost recovery, has been self funding.

²⁴ The Gowers Review of Intellectual Property was an independent review of the copyright law of the United Kingdom focusing on 'intellectual property rights', conducted from December 2005 to December 2006. The Gowers Funding Grant was issued to each local authority in England and Wales as a result of the Review. The money was specifically targeted at copyright and intellectual property enforcement. Within Carmarthenshire funding was used to set up and support a sustainable ongoing project (for example, the digital enforcement strategy and forensic lab etc).

- 4.29 As part of the digital crime strategy, Carmarthenshire Trading Standards was successful in its bid to BIS to secure funding for the development and operation of the Net WISE project.²⁵ The project provided training to all authorities throughout Wales in relation to internet enforcement, the set up of suitable equipment and the resources for such work. The project further developed a toolkit for enforcement partners throughout Wales providing desktop training which included supplying key pieces of software for such investigations.
- 4.30 Since the creation of Carmarthenshire Trading Standards Digital Crime Strategy, the team has taken a number of cases, prosecuting traders for selling fake and unsafe items from clothing and DVDs to machinery and motorbikes. The team also specialises in investigating scams and frauds. It is now common for the team to investigate and enforce on a national and international basis. One example of this is a multi million pound home-working scam originating from South Wales with links throughout the United Kingdom, America, Australia, India and Sri Lanka.
- 4.31 To date the team have secured proceeds of crime confiscations in excess of £500,000 and tackled crime to the value of in excess of £10 million. The facility and the team were recognised for its work in 2009 by the Anti Counterfeiting Group²⁶ and received a Highly Commended award for its work.

²⁵ Net WISE is a DTI (now BIS) modernisation funded project aimed at developing and maintaining a coordinated approach to internet enforcement by TSS in Wales

²⁶ The Anti-Counterfeiting Group (ACG) is a not for profit trade association, recognised as a leading authority on the worldwide trade in fakes.

- 4.32 In spite of the limited resources available to TSS, 'the Internet features in 70 of 197 LATSS strategic assessments²⁷ at present',²⁸ with TSS doing what they can to combat consumer protection issues. The 'Trading Standards e-consumer protection and internet enforcement Project' baseline assessment for the period 1 April 2009 to 31 March 2010 found that 47 per cent of TSS have a stand-alone internet investigations computer, and 33 per cent of TSS have procedures in place in relation to internet based investigations.²⁹ The SELT/BIS project builds on this expertise.
- 4.33 Many respondents to the public consultation on e-consumer protection mentioned resourcing as a critical issue in terms of training, equipment and capability, with some commenting that any shortfall in funding should be met by central government. In its response to the consultation, Slough TSS commented 'It is imperative that Trading Standards services are equipped to deal with the exponential growth in internet trade and complaints about the internet. If there is a short fall, funding and training should be made available from a central source'. The Association of Chief Trading Standards Officers (ACTSO) and Trading Standards Institute's (TSI) response highlighted that 'Some local authorities are not resourced sufficiently to be able to operate at

²⁷ A strategic assessment aims to identify longer-term issues in an area, and forecasts of trends and future issues. The assessment is used to establish priorities, allocate resources, support business planning and set a control strategy containing priorities for intelligence, prevention and enforcement activities.

²⁸ Scambusters East of England, London & TSSE (SELT) consultation response

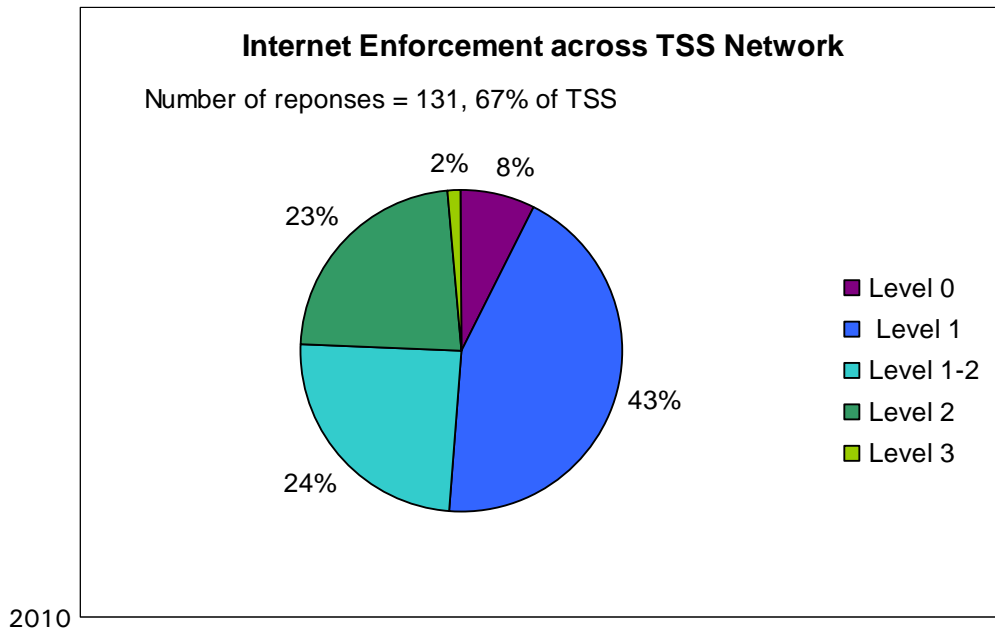
²⁹ E-Consumer Protection Project 'Trading Standards e-consumer protection and internet enforcement Project', Restricted Document. BIS have provided funding for a three year initiative which will enable trading standards to deliver a national project on the area of e-consumer protection and internet enforcement. It is being managed in partnership by the East of England, London and South East Trading Standards (SELT) authorities.

Level one.³⁰ (For a definition of the different level of capabilities see Annexe B).

- 4.34 Across the UK there is substantial variety in internet enforcement capability at a local TSS level which is a result of local prioritisation and the limited resources available to local authorities. Results from a survey carried out by the OFT show a range of capabilities across the UK TSS network.
- 4.35 More than 90 per cent of TSS operate at Level 1 internet enforcement capability or above (medium detriment, low complexity) performing targeted websweeps, undertaking test purchases and verifying compliance. Two TSS operate at Level 3 internet enforcement capability (high detriment, high complexity enforcement cases, often with a significant international component). Around eight per cent of TSS have no internet enforcement capability, instead they have agreements in place with other teams or organisations when internet enforcement is necessary. Most TSS contacted have plans in place for further development of their internet capability, or intend to purchase equipment, although some respondents were concerned about the impact of budget and staff cuts.

³⁰ Quoted from the consultation response to the strategy for protecting consumers online of The Association of Chief Trading Standards Officers and Trading Standards Institute.

Diagram 2 Internet Enforcement Capability across the TSS Network, November



Source: Self-assessed capability based on a questionnaire sent to all TSS, November 2010, response rate 67 per cent, total responses 131

Coordinate Enforcement and Investigations

4.36 The need for increased coordination (facilitated partly through intelligence sharing) was another strong theme across both workshops and responses to the consultation. Currently, coordination is achieved informally, using contacts throughout the UK and working with the RIO network, or working with TS Interlink.³¹ However it was recognised that the need for increased coordination would become more important as more TSS become active in internet enforcement.

³¹ TS Interlink is an online secure communications and information service which allows access to a variety of databases (including Companies House), news services via RSS feeds and an integrated messaging system connecting every TSS, all other Local Government Regulatory Services and other Government bodies (including OFT).

- 4.37 At an international level, the OFT is supporting the development of the ICPEN country directory of regulators and enforcers, which we will expand to include countries outside the ICPEN network.
- 4.38 Within the UK, the Welsh Heads of Trading Standards have recently formed the 'WWhoTS E-Consumer Protection Group'. Part of the group's remit will be to consider the future of Net WISE, a DTI (now BIS) modernisation funded project aimed at developing and maintaining a coordinated approach to internet enforcement by TSS in Wales.

Promoting compliance

Providing guidance to businesses

- 4.39 In May 2010, the OFT published the 'Consumer Law and Business Practice: Drivers of Compliance and Non-Compliance' report which set out to improve our understanding of the factors which drive business compliance with consumer protection law.³² The findings of the work indicate that access to clear and easy-to-apply guidance on how to comply is a significant factor in whether a business complies with consumer protection legislation. Key findings of the research included:
- businesses often have a limited understanding of the law, and small to medium enterprises (SMEs) in particular are likely to have low awareness of the detail of consumer protection laws, or how they can access relevant information to assist compliance
 - businesses want and need support and guidance to comply. Some businesses reported that support can sometimes be inconsistent and identified some guidance material as not sufficiently user friendly or accessible

³² 'Consumer Law and Business Practice: Drivers of compliance and non-compliance', OFT1225a, May 2010, www.offt.gov.uk/shared_offt/reports/Evaluating-OFTs-work/OFT1225.pdf

- businesses often use the internet to access materials, frequently using search engines to access information, rather than navigating directly to sources of advice.

4.40 In February 2010, the OFT's consultation on the development of the Sale of Goods Act Hub highlighted that business guidance needed to:

- be flexible, to meet the varying informational needs of different sized retailers
- be adaptable, so that information could be slotted into businesses existing compliance materials
- give clear examples of how business should deal with the more tricky areas of the law
- be visual, friendly, clear, brief and written in plain English
- be consistent no matter which body, government or trade, was providing the advice.

4.41 Responses to the OFT's e-consumer protection consultation indicated that key reasons for businesses not using guidance on how to comply with consumer protection legislation include lack of awareness of the guidance available and competing priorities upon businesses' time. A number of respondents indicated that businesses that are offered a commercial advantage through compliance (or a commercial disadvantage through non-compliance) will be more likely to make use of available guidance.

4.42 Consultation responses also indicated that a single source of business guidance, or a single conduit through which businesses could access the range of business guidance available, would promote the use of guidance by businesses.

4.43 A number of consultation responses also indicated that the availability of guidance that was easy to use and understand would increase the use of guidance by businesses. The OFT's guidance on the Distance

Selling Regulations³³ (albeit with some suggested improvements), the Sale of Goods Act Hub³⁴ and ERWIN³⁵ (Everything Regulation, Whenever It's Needed) were identified by respondents as being good examples of such guidance materials.

Targeted compliance checks

- 4.44 In December 2007 and again in March 2009, the OFT worked with TSS to carry out web sweeps of internet shopping websites to assess levels of compliance with consumer protection legislation. A comparison of the findings of the two web sweep exercises found that overall assumed compliance and information provision by online businesses had improved and that fewer sites were imposing unlawful restrictions on cancellations. While a greater proportion of sites reviewed in 2009 – 21 per cent compared to 17 per cent in 2008 – appeared to comply on all aspects of consumer protection legislation, there is clearly scope for further improvement.³⁶
- 4.45 Furthermore, research at EU level indicates that there is a significant gap between businesses' perception of how well they think they comply and how well they actually comply.³⁷

³³ www.offt.gov.uk/shared_offt/business_leaflets/general/oft698.pdf

³⁴ www.offt.gov.uk/business-advice/treating-customers-fairly/sogahome/

³⁵ ERWIN (Everything Regulation, Whenever It's Needed) is a website that offers guidance and information on all aspects of Trading Standards related information to retail businesses across England and Wales: www.everythingregulation.org.uk/

³⁶ 'Monitoring the internet shopping market: Assessing changes to consumer awareness and business practices in the market following OFT work', OFT1153, January 2010, www.offt.gov.uk/shared_offt/reports/Evaluating-OFTs-work/oft1153.pdf

³⁷ 'The Consumer Markets Scoreboard, 3rd Edition', European Commission, 2010, page 5: 'Although, at the EU level, 83 per cent of retailers considered themselves to be well informed about consumer legislation, only 23 per cent of them were able to correctly indicate the length of cooling-off periods for distance sales and only 26 per cent knew the legal requirements for

- 4.46 These findings indicate that there would be value in undertaking future web sweeps to continue to maintain an up-to-date picture of compliance levels among online businesses and to inform the development of business guidance.
- 4.47 Responses to the consultation supported the continuing use of web sweeps to identify non-compliance with follow up action taken by the OFT and/or TSS where appropriate.

Working with trade associations, online platforms and industry players to promote compliance, share intelligence, and resolve problems

- 4.48 Working well with industry is a critical part of how OFT addresses consumer problems and helps us to take a balanced and proportionate approach to making markets work well. When appropriate, it can give our work greater reach than taking individual cases and produce a more successful outcome for the resources available.
- 4.49 The development of effective communications channels with industry can, for example, facilitate the sharing of information regarding the nature of issues affecting the interests of consumers and ways of best addressing those issues. Such cooperation is mutually beneficial since, where such issues can be effectively tackled, businesses themselves benefit from greater consumer confidence over the long-term.
- 4.50 Consultation responses showed strong support for the initiation and maintenance of channels to facilitate prompt sharing of relevant information between industry and public authorities.

returning defective products.'

www.ec.europa.eu/consumers/strategy/docs/3rd_edition_scoreboard_en.pdf

Tackling spam

- 4.51 Responses to the consultation indicated that the global nature of spam means that an international approach is essential, with one overall government agency taking the lead for the UK.
- 4.52 The OFT will continue to work with partners and take action to help ensure that consumers are educated about how to avoid falling victim to scams and rogue traders. The OFT will also continue to play a central role in the functioning of the London Action Plan (LAP), an innovative and ground-breaking coalition between government agencies and industry to combat internet related threats to the economic welfare of consumers, with a particular focus on spam and viruses. Independent research has shown that there is a correlation between countries that participate in the LAP and lower levels of cyber related threats to consumers.

Empowering Consumers

Educate consumers

- 4.53 Consumers are less likely to understand and therefore are less likely to enforce their consumer rights when buying online than when buying offline. This has important implications for fully effective internet markets, which need informed consumers to help encourage innovation and competition.
- 4.54 Furthermore, there is often confusion as to the difference between online and offline rights. In 2010, BIS carried out a survey as part of the Know Your Rights campaign, which showed that three quarters (77 per cent) of UK consumers don't know that there are differences between online and offline consumer rights. It also showed that more

than one in 10 (13 per cent) of consumers admit to being unsure of their consumer rights with online purchases.³⁸

- 4.55 Some aspects of consumer rights are better understood than others. According to the Attitudes to Online Markets (2010) survey,³⁹ 80 per cent of internet users (based on 1085 responses) know that it is possible to claim their money back from a credit card company if the goods or services are not delivered (section 75 of the Consumer Credit Act 1974 applies to goods costing between £100-£30,000). However, 35 per cent of internet users were unaware that they would be entitled to a refund if an item they purchased online was not delivered by the agreed date or within 30 days of the order (Regulation 19(5) of the DSRs). Twenty-four per cent of internet users (based on the same sample size) were also not aware of the seven-day cooling off period for most online purchases. This result came from the respondents identifying 'true or false' to a number of statements. It is likely that without prompting, awareness of rights may be lower.
- 4.56 There are various innovative channels and techniques that can be effective in targeting different types of consumers with messages that are relevant to them. For example, during the February 2009 'Scams Awareness Month' campaign, the OFT launched two spoof websites to warn consumers of the dangers of 'miracle' health and weight loss scams that cost UK consumers an estimated £20 million every year. The sites mirrored the type of spoof sites that scammers adopt and they attracted 15,000 unique visitors.
- 4.57 One of the issues identified during the evidence review and consultation was the number of conflicting messages being delivered to consumers. The consultation and follow-up workshops demonstrated very high levels of support for developing a common set of consumer messages so that different organisations give consumers

³⁸ www.bis.gov.uk/news/topstories/2010/Nov/how-to-be-savvy-when-doing-your-christmas-shopping

³⁹ Attitudes to Online Markets (OFT1253), FDS, August 2010.
www.of.gov.uk/shared_of/consultations/eprotection/oft1253

consistent advice. There was also consensus that these would have to be communicated by using low cost education channels wherever possible. In addition, it was acknowledged that having business support would be beneficial.

- 4.58 Educating consumers was seen as a high priority from a number of those consulted. This would enable both consumers and businesses to know what consumer protection is available. However a number of consultation respondents stated that care needs to be taken during any educational campaigns not to scare consumers away from using the internet and that priority should be given to provide positive stories.
- 4.59 We received a number of responses that considered education through schools and adult education courses to be the most effective way of getting safety online messages to consumers.

Improve security and transparency of transactions

- 4.60 Many consumers use the internet to search for goods and services and compare prices, but do not then complete the process by going on to make an online purchase. While there are a range of reasons for this behaviour (for instance the desire to gain further information from sales-people or the need to physically view or try the good), in many cases it results from consumers' concerns about entering personal or financial details online, or paying in advance of receiving goods.
- 4.61 The Attitudes to Online Markets (2010) research indicates that, among internet users who haven't bought online in the last year, concern about the security of financial details is the most important reason for not buying goods and services online (33 per cent, based on 365 responses).⁴⁰

⁴⁰ Attitudes to Online Markets (OFT1253), FDS, August 2010.
www.of.gov.uk/shared_of/consultations/eprotection/oft1253

- 4.62 Perceptions of risk for some consumers and some payment methods are unduly high. In 2009, reported internet/e-commerce fraud loss in the UK decreased by 15 per cent⁴¹ from 2008, whilst internet transactions increased by 14 per cent⁴² during the same period. The difference between perception and reality is often stark. Perceptions eventually lead to myths which are difficult to dispel. For instance the Home Office claims that there is unjustified fear of crime: 'In spite of the significant falls in the main volume crimes in recent years, almost three-quarters of the public still believe that the national crime rate has been rising.'⁴³
- 4.63 The general view from our consultation was that businesses are already attempting to make payment systems safer, through mechanisms such as the Payment Card Industry Data Security Standard, Verified by Visa/Secure by MasterCard, and initiatives such as consumer guides on safe payments. Education was seen as the strongest way of encouraging consumers to transact more safely, although the focus needed to be on the positive steps that consumers could take to keep themselves safe, rather than on sensational stories of problems that consumers may encounter.
- 4.64 One response to the consultation highlighted the importance of business and industry involvement in education, providing content (for example a brief description on the levels of protection applicable to different payment mechanisms) and potentially helping to deliver some of the messages.

⁴¹ UK Cards Association, 2010, 'Fraud the Facts 2010', www.theukcardsassociation.org.uk/files/ukca/fraud_the_facts_2010.pdf

⁴² IMRG/Cappgemini Sales Index, January 2010. [www.imrg.org/8025741F0065E9B8/\(httpPressReleases\)/546442736834C8CE802576B200597E8A?OpenDocument&view=archive](http://www.imrg.org/8025741F0065E9B8/(httpPressReleases)/546442736834C8CE802576B200597E8A?OpenDocument&view=archive)

⁴³ Crime in England and Wales 2002/03, <http://rds.homeoffice.gov.uk/rds/pdfs2/hosb703.pdf>

Leverage learning and improve consumer redress

4.65 Despite the widely reported benefits of shopping online, consumers do from time to time encounter problems. In a survey conducted by FDS International in January 2010, one in seven consumers who buy goods on the internet (14 per cent, based on 735 responses) has experienced a problem when buying a good or service online. Of these, 37 per cent (based on 112 responses) stated that they had had their confidence knocked by this experience and claimed to use the internet less as a result.⁴⁴

Leverage learning

4.66 People can be more effective as consumers, and derive greater benefits from transacting when they are well informed about the choices available. The internet has significantly reduced search costs and improved the ability to make comparisons between products. In general, this competitive pressure increases the incentives for companies to innovate or reduce prices.

4.67 However, the internet also creates barriers for consumers, including unnecessarily complex products and services, larger numbers of unknown firms and intangible transactions. These barriers can be reduced where consumers share learning via dedicated sites or use dedicated feedback systems. In response to the provision of such systems, there is a risk that some businesses may pay individuals for positive feedback without making this arrangement clear to consumers.⁴⁵ Firms may also attempt to protect their reputation by seeking to remove feedback which they consider to be illegitimate with threats of defamation action against website owners or ISPs.⁴⁶

⁴⁴ Attitudes to Online Markets (OFT1253), FDS, August 2010.
www.ofc.gov.uk/shared_ofc/consultations/eProtection/ofc1253

⁴⁵ A practice which is prohibited under paragraph 11 of Schedule 1 of the CPRs.

⁴⁶ www.bbc.co.uk/news/uk-wales-north-west-wales-11373722

4.68 In many instances consumers only check for known problems about a trader after a problem has occurred, rather than in advance of the transaction. Feedback systems and review sites may be able to help consumers to judge the trustworthiness of a trader and the likely quality of goods and services if they use them in advance of a purchase.

Improving consumer redress

4.69 Consumer redress is another area where issues have been identified. Consumers are often unclear where to go to seek help, firms are often unclear of their responsibilities and the legal framework could also be made more effective.

4.70 If things do go wrong, consumers are not always confident of where to go for help. When asked in the survey who they would turn to in the event of a dispute, at least 16 different answers were given (see diagram 3 below). A quarter of consumers who buy goods on the internet (26 per cent, based on 735 responses) stated that either they did not know who to turn to or they would not turn to anyone else in the event of a dispute with an online seller.⁴⁷

www.telegraph.co.uk/travel/travelnews/7994817/TripAdvisor-faces-legal-action-from-upset-hoteliars.html

www.telegraph.co.uk/technology/internet/8143814/Mumsnet-founders-demand-libel-law-reform.html

⁴⁷ Attitudes to Online Markets (OFT1253), FDS, August 2010.
www.oft.gov.uk/shared_oft/consultations/eProtection/oft1253

Diagram 3 Who consumers turn to in the event of a with a dispute with an online seller



Source: 'Attitudes to Online Markets' (OFT1253), FDS, August 2010.

www.offt.gov.uk/shared_offt/consultations/eProtection/oft1253

4.71 From the graph above, consumers do seek redress from their credit card companies. It is likely that consumers in these cases are relying on Section 75 Consumer Credit Act (CCA) 1974. This legislation provides that consumers who use their credit card to make purchases of over £100 but less than £30,000 may make a claim against their credit card company for any breach of contract or misrepresentation by the trader. This legislation provides that where the cash price (purchase price) of a single item is more than £100 and does not exceed £30,000, the consumer can hold the trader and/or the credit card company liable for any breach of contract or for any misrepresentation by the trader.

- 4.72 This is an important avenue for redress, and a strong lever by which (along with other redress mechanisms provided by payment service providers) consumers' confidence online can be enhanced. This is not only because s. 75 provides an easy solution for consumers when things go wrong, but also it addresses the issue of the lack of a bricks and mortar presence (the problem of 'can you trust an internet based trader?'), because the card company does know who the trader is, as they have a relationship with them. This means that even if the consumer cannot get redress from the trader, they can get redress from the card provider, and the card provider is in the best position to recover their losses from the trader.⁴⁸ S.75 is a good example of this balance working in practice.
- 4.73 Another identified problem is the lack of an effective legal framework for consumers to obtain adequate compensation for mass claims. There are limitations with the current system of the UK Group Litigation Orders whereby each claimant files a separate claim form and is entered upon a group register. Such Orders are used more as a case management tool for the courts by merely grouping together similar claims. In addition, such systems do not take into consideration the cross-border element of many transactions.⁴⁹
- 4.74 There are currently a number of mechanisms consumers can use to seek redress for online issues, such as local TSS, industry associate schemes (such as IMRG or Safebuy) or an Ombudsman service (such as the Financial Ombudsman Scheme).
- 4.75 Under the Europe 2020 Strategy, the European Commission (EC) has proposed a Digital Agenda for Europe. This proposal aims to 'better

⁴⁸ The consumer is able to claim redress under section 75 Consumer Credit Act (CCA) if they have made a full or partial payment for the goods or services using their credit card. This will only apply if it the type of credit card which allows the consumer the option of making more than one repayment, for example, by monthly payments. Credit cards which require the balance to be paid in full in one payment will not be covered here

⁴⁹ www.ofc.gov.uk/shared_ofc/reports/ofc_response_to_consultations/ofc1100.pdf

exploit the potential of Information and Communication Technologies (ICTs) in order to foster innovation, economic growth and progress.⁵⁰

- 4.76 This Agenda aims to improve consumers' trust around the security of payments and privacy. The EC is looking to review the EU data protection regulatory framework. It also intends to publish a clear and accessible online Code to explain consumers' rights in the digital world. This Code will also include contract law, and EU-wide online dispute resolution. The EC also envisages introducing an EU online trustmark to guarantee consumer protection.
- 4.77 In October 2009 the EC carried out a study on the use of Alternative Dispute Resolution (ADR) in the European Union.⁵¹ It found that there are 750 different schemes across Member States and the use of ADR in the EU has been increasing. In 2008 there were approximately 530,000 individual cases compared to 410,000 in 2006, and 473,000 in 2007. ADR schemes are often sector specific and usually cover financial services, package travel and telecommunications industries.
- 4.78 The study highlighted some best practice schemes currently in place including ones in France, the Netherlands and Austria. In France, the 'France Mediateur du Net' established an online dispute resolution service in 2004. The Netherlands also offers a similar scheme, which is partly funded by the Dutch Ministry of Justice, as does the Austrian Internet Ombudsman, which was founded in 1999.
- 4.79 The study concludes that the EC should consider producing EU-wide guidelines which could be implemented into national guidelines or standards.
- 4.80 In responses to our consultation and at various workshops, there was a general consensus on the need to develop a single online complaints system where consumers can report all online problems. This was seen by some respondents as a priority.

⁵⁰ www.europa.eu/legislation_summaries/audiovisual_and_media/si0016_en.htm

⁵¹ ec.europa.eu/consumers/redress_cons/adr_study.pdf

4.81 The majority of respondents agreed that ADR processes may be beneficial for consumers to seek redress, but concerns over administering these processes were high. There were suggestions that the current schemes available should be looked at further to ascertain the impact these have had and to monitor EU developments in this area.

5 ACTIONS – DEVELOPING MORE EFFECTIVE ENFORCEMENT

- 5.1 Significant progress has been made in developing an effective e-enforcement capability across the UK, and in the wider e-enforcement landscape. The Police Central e-crime Unit (PCeU) was established in October 2008 to create a national centre of excellence to combat e-crime in England, Wales and Northern Ireland. A year later the OFT established its Internet Enforcement team, focusing on protecting the economic interests of consumers.
- 5.2 The Office of Cyber Security and Information Assurance (OCSIA) alongside the Cyber Security Operations Centre (CSOC) work with lead government departments and agencies such as the Home Office, Ministry of Defence (MoD), Government Communications Headquarters (GCHQ), the National Technical Authority for Information Assurance (CESG), The Centre for the Protection of National Infrastructure (CPNI) and BIS in driving forward the cyber security programme for UK government.
- 5.3 Regional centres have been established across the UK. e-Crime Wales was set up in 2004, and brings together the four Welsh Police Forces, specialist public sector organisations and expert commercial businesses. In Scotland, e-Crime Scotland has been developed through the auspices of the Scottish Financial Crime Group together with key partners in the Scottish Business Crime Centre, Scottish Law Enforcement, Scottish Government and the wider business community.
- 5.4 Other regional and local centres of expertise for e-consumer protection have been developed across the UK, including at least two TSS conducting investigations at Level 3 capability (high detriment, high complexity) and around one in four (23 per cent) able to conduct investigations at Level 2 (medium/high detriment, medium complexity).
- 5.5 A BIS funded three-year project, 'e-Consumer protection and internet enforcement', undertaken by SELT on behalf of TSS is focused on improving coordination, intelligence and capability (including the provision of training and equipment across TSS). The project carried

out a survey to inform a gap analysis across TSS, ensuring that suitable training and equipment could be provided to those local authorities who were in most need. This on-going project, currently due to finish in 2012, is helping to build capability within the TSS across the UK.

- 5.6 ACPO developed an e-Crime strategy in May 2009. The Home Office is working on a cyber-crime strategy, which it plans to publish in early 2011. The National Fraud Authority (NFA) launched in October 2008 to bring together the numerous counter-fraud initiatives that existed launched Action Fraud (AF) in October 2009. Action Fraud's role is to co-ordinate the fight against fraud in the UK. NFIB (National Fraud Intelligence Bureau) was also launched in October 2009.⁵²
- 5.7 This investment in capability and infrastructure, particularly that relating to e-consumer protection (the focus of this strategy) could be made even more effective by improving data-sharing and intelligence, developing internet enforcement capability, and increasing the coordination of enforcement.

Improving data-sharing and intelligence

- 5.8 The OFT is working towards sharing data and intelligence internationally. The OFT has information sharing and enforcement Memorandum of Understanding (MoUs) with a number of overseas agencies, such as the US Federal Trade Commission (FTC) and the Australian Competition and Consumer Commission (ACCC), which facilitates protection of UK consumers where the trader is based overseas.
- 5.9 Given the immense value to the UK and other international enforcers of sharing internet data globally, we are also liaising with the Information

⁵² The NFIB uses reports of fraud to help catch serial fraudsters and provide a better picture of the nature of fraud. The Bureau is government-funded and run by the City of London Police, which is the National Lead Force for fraud, in partnership with police forces and the public and private sector

Commissioners Office (ICO) and the Ministry of Justice (MoJ) over the legal constraints surrounding sharing consumer complaints information (see Action 5.iii). Sharing intelligence and complaints data more widely will increase the effectiveness of enforcement (both our own, and that of others), enable us to more quickly identify emerging harmful business models, and enable enforcers to more effectively prioritise work and identify cases with high consumer detriment.

- 5.10 At a national level, alongside the Regional Intelligence Units and TSS we are rolling out a nation-wide IMD to facilitate intelligence sharing amongst consumer protection agencies. It may well be possible to use the same system for internet intelligence. However investigations of internet cases generate substantial quantities of data automatically via a range of software programmes and other sources. Therefore any intelligence system selected must be cost effective in terms of automated data input from other sources. This will obviously be a factor in determining a viable e-intelligence system for the UK (see Action 5.i).
- 5.11 We also work proactively with the police to share evidence and assist prosecutions. We have a number of MoUs with national bodies such as the Serious Organised Crime Unit (SOCA), HM Revenue and Customs (HMRC), the Financial Services Authority (FSA) and the Police, and are in talks with the NFIB to share Consumer Direct data (see Action 5.ii). Data-sharing with the NFIB received strong support from TSS, SOCA, and Local Government Regulation (LGReg) during enforcement workshops we held.

Improving data-sharing and intelligence: Initiatives	Lead agency and key partners
<p>PRIORITY</p> <p>5.i Improve data-sharing and intelligence between and amongst the OFT and TSS by developing an e-intelligence system (possibly using IMD⁵³) and building national intelligence capability (which could include leveraging and supporting the Regional Intelligence network)</p>	<p>OFT, BIS and TSS, and LGR</p>
<p>PRIORITY</p> <p>5.ii Contribute to national data-sharing, working with NFIB and other agencies to share intelligence and Consumer Direct data</p>	<p>OFT/TSS, NFIB</p>
<p>5.iii Work towards sharing consumer complaints data globally for example via Consumer Sentinel⁵⁴</p>	<p>OFT, BIS, LGR and Citizens' Advice</p>

Develop Internet Enforcement Capability

5.12 The OFT established its Internet Enforcement team in October 2009, employing staff with specialist technical expertise and developing an Internet Lab. The Lab has forensic and secure storage of evidence gathered online and on traders' premises, stand alone computers, and

⁵³ IMD – Intelligence Management Database (currently used by all Regional Intelligence Officers across the UK, the OFT and around 35 per cent of TSS).

⁵⁴ Consumer Sentinel provides law enforcement members with access to consumer complaints provided directly to the U.S. Federal Trade Commission by consumers, as well as providing members with access to complaints shared by data contributors.

software for improving the effectiveness of OFT investigations online. The Lab is further leveraged by a network of national and international contacts, and strong legal expertise.

- 5.13 The Internet team has built a significant internet investigation and enforcement capability, which has produced a range of completed cases, details of which are available on the OFT's website.⁵⁵ In doing so, the team has obtained undertakings and has also taken other action (for example engaging with domain name registrars in respect of websites of concern) where appropriate.
- 5.14 The team currently has a number of ongoing investigations into online practices which the OFT has prioritised for investigation, building on the experience gained since the team was established. For example, it is currently investigating a variety of deceptive online marketing and advertising practices and also unfair trading practices by traders not complying with their legal obligations. Information on future completed investigations will be made available on the OFT's website.
- 5.15 A number of TSS or regional groupings of TSS, and TSS in partnership with other organisations have developed strong internet enforcement capability, and have links to local police forces, NFIB and industry.
- 5.16 However differing local priorities and funding constraints mean that not all TSS are equipped to deal with online problems. Furthermore, as the internet is not based around local geographies, there is not necessarily a clear local need for all TSS to develop an internet enforcement capability.
- 5.17 What is required is clarity over which groups are responsible for taking e-consumer enforcement action in the UK, and how they should be funded, given they are acting for the benefit of all TSS. Under current funding arrangements, those TSS with internet expertise may be expected to focus their resource on protecting consumers within their

⁵⁵ www.of.gov.uk/OFTwork/consumer-enforcement/

own jurisdiction rather than those for which another local authority is responsible, although a number of options currently exist for co-operative arrangements and work sharing.

- 5.18 Concentrating resources and expertise in a limited number of groups is likely to be the most cost effective way of providing e-consumer protection across the whole of the UK. Ideally, this would be supported by an effective intelligence network and tasking system. The cost effectiveness results from the significant economies of scale that can be exploited: there are large fixed costs in developing an internet lab due to large capital investment requirements, and related costs in terms of training staff, coordinating, and liaising with other enforcers, government agencies and international bodies. However undertaking additional investigations adds very little incremental cost (if the initial system was correctly scoped).
- 5.19 In addition there are a number of initiatives underway that could be exploited more widely across the UK, including OFT's work with the Consumer Protection Cooperation Regulation (CPC) network, and the development of a UK internet investigation manual. The OFT has plans to develop an Internet Portal to enable data, intelligence and know how to be shared between CPC members, this could be extended to include TSS. With additional funding the Internet portal might be a useful platform to house a co-ordinating mechanism for UK e-consumer enforcement action.
- 5.20 The CPC work includes the development of a website to act as a repository to share knowledge of experience and best practice by Member States, and know-how sharing workshops. Currently three workshops are in detailed planning: i) enforcement experiences and applying the law: ii) technical skills and equipment: and iii) emerging threats and working with industry.
- 5.21 It is envisaged that the CPC website will include minutes of the know-how workshops, detail on agencies' powers and the remedies available to them, contacts details of internet investigators, relevant national court decisions, precedent letters, undertakings, case summaries and

such other information as is decided will be of use. The CPC website is likely to be linked to the UK Internet Portal, providing access for TSS.

5.22 During the consultation, some organisations and individuals commented on a range of possible abuses using '.uk' (including '.co.uk') domain name. Nominet is already aware of these potential issues, and is currently consulting with stakeholders on 'Dealing with domain names used in connection with criminal activity'. In addition, the OFT and Nominet have begun to work together to improve awareness of, and ability to respond to, abuses using '.uk' domain names.

Developing internet enforcement capability: Initiatives	Lead agency and key partners
<p>PRIORITY</p> <p>5.iv Build web portal for TSS & CPC networks to enable capability sharing. Migrate enforcement tools (such as manuals and pro-forma letters) to portal.</p>	OFT, TSS and LGR
<p>5.v Work with TSS and other key players to develop a small number of dedicated, expert teams, within TSS to develop UK wide internet coverage. Invest in critical infrastructure for key TSS</p>	BIS, OFT, TSS, TSI, LGR
<p>5.vi Take strategic enforcement action to clarify UK internet case law (including key issues such as intermediary liability, redress for consumers, the legal status of digital products and the application of the CPRs to emerging trading practices) to ensure internet markets function effectively and TSS can build on legal action</p>	OFT
<p>5.vii Work with Nominet to improve awareness of, and ability to respond to, abuses using '.uk' (including</p>	OF/Nominet

Coordinate enforcement action

- 5.23 The OFT aims to operate as a central hub for intelligence sharing and case management between TSS, police and other enforcement agencies. Without central coordination and intelligence sharing, there is a significant risk of duplication of investigation, and potential for interfering with other agencies' investigations. This is a particular risk where the police are investigating, or where there is a risk of compromising a prosecution.
- 5.24 The OFT has recently initiated work to facilitate and coordinate TSS enforcement action following the OFT's investigation into the misleading selling of European Health Insurance Cards. As part of this work, the OFT is sharing intelligence with various TSS, in particular relating to websites that may be engaged in the misleading selling of other services that are freely available direct from government. In doing so, the OFT will share and discuss examples of best practice from its enforcement action against the misleading selling of European Health Insurance Cards, for example text from undertakings obtained in that case.
- 5.25 Given the global nature of the internet, international co-operation is an important element of our online enforcement activity and we regularly liaise with overseas agencies during our work. For example, we work with agencies in other European Union Member States as part of the CPC and also international agencies via ICPEN.
- 5.26 In a CPC context the OFT recently took action against an operator of bogus investment websites. Evidence available to the OFT indicated that UK consumers who invested money in the trader's investment plans subsequently received no return on their investments despite the trader 'guaranteeing' a return. Also, consumers were unable to contact the trader using the details provided on its website which included a false UK address. Following concerns expressed by the OFT to the Internet Service Provider (ISP) hosting this trader's website, the

website was suspended. During its investigation the OFT identified a second website, which it thought was also offering bogus investment opportunities, which also appeared to be operated by this trader. Evidence available to the OFT indicated that funds flowing from this activity were being sent by the trader's payment service provider to individuals in another European Member State. As a result, the OFT made a CPC referral to the relevant agency in this European Member State.⁵⁶

- 5.27 More widely, the OFT assisted the FTC, an ICPEN partner, as part of the FTC's ongoing investigation into a US company that the FTC alleges deceptively sold electronics to UK consumers, including via the use of websites ending in '.uk'.⁵⁷ As part of this work it came to the OFT's attention that some UK consumers who purchased items from websites operated by this US company may have been incorrectly refused a chargeback request by their banks. In light of this, the OFT wrote to UK consumers that complained to the OFT or the FTC to advise them of their chargeback rights in relation to goods purchased from websites operated by this US company. The letter also provided information on consumers' chargeback rights and the procedure that certain consumers could follow if they wished their chargeback request to be considered afresh.
- 5.28 OFT is currently leading a workstream at ICPEN, developing a country directory including information on contact details, remits and other working practices for regulators and enforcers to help facilitate inter-agency coordination.

⁵⁶ For more details see www.oft.gov.uk/OFTwork/consumer-enforcement/consumer-enforcement-completed/online-trader-investigation/

⁵⁷ More information on the FTC's investigation can be found at www.ftc.gov/os/caselist/0923081/index.shtm

5.29 We also coordinate with other UK agencies. TSS and the OFT currently make use of TS Interlink, or coordinate informally either through the RIO network, or by email.

Coordinate enforcement action: Initiatives	Lead agency and key partners
<p>PRIORITY</p> <p>5.viii Investigate mechanisms for co-ordinating enforcement action between TSS and OFT, potentially build on the Web portal (see 5.iv) as a site for coordinating enforcement action</p>	<p>OFT, TSS, CPC network, LGR</p>
<p>5.ix Clarify remits of OFT and TSS, develop links and informal coordination mechanisms with other law enforcement agencies</p>	<p>OFT, TSS, LGR</p>
<p>5.x Further develop national and international coordination function, liaising with national and international regulators and enforcers</p>	<p>OFT</p>

6 ACTIONS – PROMOTING BUSINESS COMPLIANCE

- 6.1 This section sets out actions to be taken to promote business compliance with consumer protection legislation, including by ensuring that businesses are clear about where to go to for advice, that the guidance that businesses receive meets their needs, and that enforcement authorities work effectively with industry to identify and address consumer problems.

Inform business

Providing guidance to businesses

- 6.2 In order to build upon the findings of the OFT's 'Consumer Law and Business Practice: Drivers of Compliance and Non-Compliance' research (see paragraph 4.39, page 25 above), the OFT is exploring in greater detail the following factors relating to the provision of guidance to businesses:
- how the OFT and TSS can support stakeholders to deliver messages to businesses, especially SMEs, on consumer protection laws and consumer rights
 - how businesses (especially SMEs) access information and how we can raise awareness levels of the consequences of breaching consumer protection laws
 - how to improve businesses' awareness of the laws and regulations that are hard to understand or contain difficult detail
 - how to harness the business desire to build and maintain reputation, and their intuitive approach to fairness, in order to raise the awareness and priority of consumer protection laws.
- 6.3 Going forward, the OFT will continue to develop and improve its provision of business guidance in light of emerging findings from this ongoing work.

- 6.4 Specifically, the OFT has identified and begun delivery of a number of initiatives aimed at improving the availability and utility of guidance to businesses, including those that trade online.
- 6.5 In September 2010, the OFT launched the Sale of Goods Act (SOGA) hub,⁵⁸ which provides free online materials that retailers can view or download. Developed in consultation with business and trade associations, the hub provides a range of training and promotional materials for retailers to help sales staff understand their legal obligations and improve customer service. The hub is currently being publicised to business and being evaluated.
- 6.6 In November 2010, the OFT began utilising the same process undertaken in the development of the SOGA hub to develop advice for business on the Consumer Protection (Distance Selling) Regulations 2000 ('DSRs').
- 6.7 As part of the government web convergence project, by March 2011 the OFT will ensure that content available for business on the OFT website is available on, or accessible from, the Business Link website.⁵⁹
- 6.8 In May 2010 the OFT launched a re-designed website and the OFT is now undertaking a review of all website content. The content review aims to ensure content is user friendly, relevant for the target audience, accessible and optimised for the web (including search engines).

Targeted compliance checks

- 6.9 During 2010, the OFT has taken part in an EU-coordinated web sweep of ticketing websites and a web sweep into online marketing and advertising to children and young adults which was coordinated by

⁵⁸ www.oft.gov.uk/business-advice/treating-customers-fairly/sogahome

⁵⁹ www.businesslink.gov.uk/bdotg/action/home

ICPEN. As a result of these sweeps a number of websites of concern were identified which were fed back to the sweep coordinators.

- 6.10 The OFT will continue to periodically undertake web sweeps in order to assess and identify non-compliance by internet shopping websites. Where appropriate, the OFT and TSS will follow up on the websites by informing relevant businesses of any requirements with which their sites do not comply and directing the businesses to relevant guidance materials.

Inform business: Initiatives	Lead agency and key partners
<p>PRIORITY</p> <p>6.i Continue to improve guidance and sign-posting for businesses to ensure they have access to clear, relevant information – leveraging Business Link and initiatives such as Sale of Goods Hub.</p>	<p>OFT, Industry, TSS (ERWIN)</p>
<p>6.ii Continue to check for compliance, inform non-compliant businesses and direct to guidance materials.</p>	<p>OFT and TSS</p>

Cooperate with businesses

Clarifying level of consumer protection for C2C transactions

- 6.11 The OFT has recently liaised with key online platforms regarding their procedures for differentiating between traders who are operating as consumer-sellers and those who are operating as businesses and for ensuring that those who are businesses comply with the extra requirements of consumer protection legislation that apply to them.
- 6.12 We will continue to work with online platforms to ensure that:

- they have effective mechanisms in place to identify traders who are operating as businesses and to ensure that such traders comply with relevant consumer protection legislation
- consumers are able to identify whether a trader is operating as a business or as a consumer-seller
- consumers have access to information regarding the different levels of protection that apply to their transaction depending on the status of the trader that they are buying from.

Providing guidance to web designers

- 6.13 Web design agencies often play a key role in determining how online businesses engage with their consumers. By working with web design agencies, the OFT can help ensure that compliance is 'built-in' to websites used by online businesses.
- 6.14 The OFT will target web design agencies with appropriate guidance which explains why they should know about the law and how they can ensure that the sites that they design are compliant.

Reinforcing consumer feedback mechanisms

- 6.15 Consumer feedback mechanisms, such as review sites and product and seller ratings, are increasingly prevalent on the internet. For a growing number of consumers they constitute an important resource for researching potential purchases, informing decisions and avoiding potential detriment.
- 6.16 The utility of these mechanisms depends on the ratings and reviews reflecting the genuine opinions of consumers. In the event that, for example, a trader uses a review mechanism to post information which could mislead consumers or where a trader takes action to remove unfavourable, but genuine, consumer reviews, consumers' interests are likely to be harmed.

- 6.17 Where appropriate, the OFT will take action against such practices to ensure that consumers continue to benefit from genuine consumer reviews and ratings on the internet and are not misled by fake reviews.
- 6.18 The OFT is keen to explore with BIS ways of encouraging the development of new consumer feedback systems.

Initiating and maintaining channels for ongoing dialogue with industry

- 6.19 The OFT's internet enforcement team has begun to initiate and develop effective communication channels with key internet platforms to ensure that the OFT has timely access to relevant information regarding trader accounts where there is evidence of consumer detriment.
- 6.20 We will continue to work with online platforms to develop and maintain these channels in order to facilitate ongoing dialogue for the purposes of horizon scanning, intelligence sharing and problem solving.
- 6.21 The OFT will also participate in, and lead on, a 'know-how' workshop with other EU consumer protection authorities to discuss experiences and best practice in working with industry to solve problems with e-consumer protection.

Cooperate with business: Initiatives	Lead agency and key partners
<p>PRIORITY</p> <p>6.iii Work with industry to ensure that:</p> <ul style="list-style-type: none"> • consumers are provided with clear information regarding the level of consumer protection for C2C transactions • website designers are provided with information which helps them to build compliance into the websites they produce for online retailers • the utility of consumer feedback mechanisms is reinforced. 	<p>OFT, TSS and Industry</p>
<p>6.iv Initiate and maintain channels for ongoing dialogue with industry for the purposes of horizon scanning, intelligence sharing and problem solving</p>	<p>OFT and Industry</p>

7 ACTIONS – EMPOWERING CONSUMERS

Educate Consumers

- 7.1 Consumers are becoming more internet-savvy. They more routinely install security software,⁶⁰ they respond less frequently to spam,⁶¹ they use their credit cards more safely online, they are more wary about extravagant claims, and they sometimes undertake research before they buy. Consumers are listening to their banks, to consumer bodies and other organisations promoting safe online behaviour. In response to the need for consumer education identified in this strategy, OFT will work to raise consumer awareness of their online rights to reinforce this progress, and, in partnership with others, encourage consumers to take further responsibility to better protect themselves online.
- 7.2 The OFT has undertaken a range of consumer awareness and education campaigns designed to ensure consumers are skilled, well informed and confident. In general, such consumers are able to operate effectively and safely within markets, and exert effective pressure on firms. In an online context, the OFT has run 'Scamnesty' as part of Scams Awareness Month⁶² in February 2010 (this campaign is run annually), and in July 2010 the 'Just Tick It' scam ticketing campaign.

⁶⁰ OxIS 'The Internet in Britain 2009', <http://microsites.oii.ox.ac.uk/oxis/> 'OxIS has found that concerns over many online negative experiences, such as spam, viruses and fraud, are not as great as portrayed in the media, and the 2009 survey reinforces the degree that users are experiencing fewer problems and are doing more to address them. That is, there is an increasingly effective self-regulation by users, such as by installing anti-virus software.'

⁶¹ The Economist, 'Long Life Spam', Nov 18 2010 'In 2008 researchers from the University of California at Berkeley and San Diego posed as spammers, infiltrated a botnet and measured its success rate. The investigation confirmed only 28 'sales' on 350m e-mail messages sent, a conversion rate under .00001 per cent. Since then, says Mr Peterson, the numbers have got worse.' www.economist.com/node/17519964?story_id=17519964

⁶² www.of.gov.uk/news-and-updates/press/2010/07-10

- 7.3 'Scamnesty', run in partnership with TSS, raised awareness of the scale of mass marketed scams.⁶³ The campaign called on consumers to drop scam mailings they received into designated bins or boxes at local libraries and other public areas throughout the UK. The campaign also raised awareness of the increasing number of scams being targeted to consumers via online channels.
- 7.4 The Just Tick It campaign focused on raising awareness of fake ticket websites. In addition it encouraged consumers to check the legitimacy of websites which is discussed in more detail under 'leveraging learning and redress' at paragraph 7.16, page 59.
- 7.5 The OFT's role in online transactions is to protect the economic interest of consumers. The focus of the OFT's educational message in this area is informing consumers of their rights when shopping online. There are a number of industry associations, Government departments and consumer and internet organisation that convey messages about staying safe online. The OFT's focus complements this.
- 7.6 Where possible, the OFT will encourage consumer protection bodies and industry to work together in order to provide consistent messages on buying and selling online and to focus on simple tips that people can remember easily. We need to ensure that consumers are not confused by mixed messages given out by multiple organisations.
- 7.7 The focus of the OFT's campaigns will be on business to consumer (B2C) transactions, highlighting the differences in consumer rights that exist for C2C transactions. Consumers have low levels of understanding as to how levels of consumer protection differ depending on who the vendor is. Occasionally this ignorance is exploited. The OFT plans to monitor developments in C2C markets and

⁶³ The OFT's definition of a mass marketed scam is 'a misleading or deceptive business practice where you receive an unsolicited or uninvited contact and false promises are made to con you out of your money'.

may in the future take action to increase understanding and consumer protection (see also paragraph 6.11, page 50 in Business Compliance) .

- 7.8 In addition to monitoring C2C transactions, there are a number of other areas where it will be important to take account of developments in internet markets. The OFT will need to monitor consumer complaints databases to identify new trends and threats and use this information to inform future consumer education campaigns.
- 7.9 With the development of social media, and other viral communications, there are now many more means of providing messages to consumers often for free or at very low cost. The OFT will investigate how these channels could be used to communicate e-protection advice, taking stock of previous examples and overseas experience, to determine the most effective channels and techniques.
- 7.10 The current Government-wide marketing and advertising freeze places a restriction on marketing activity which will need to be considered when planning communications. Any initiatives developed will need to be taken forward on a no or low cost basis, unless a sound business case for expenditure can be developed.

Educate consumers: Initiatives	Lead agency, key partners
<p>7.i Work with other organisations including government departments and consumer bodies to ensure that we are consistent in the messages we give consumers about online markets. Ensure that our communications are well planned to avoid duplication and enable maximum reach.</p>	<p>OFT, Citizen's Advice, Which? Consumer Focus, Get Safe on Line and other relevant consumer bodies</p>
<p>PRIORITY</p> <p>7.ii Develop education messages focusing on consumer rights when buying online. Disseminate messages through a range of channels, for example, through social media and other viral communications.</p>	<p>OFT, Citizen's Advice, Which? Consumer Focus and other relevant consumer bodies</p>

Improve transparency and security of transactions

- 7.11 In 1999, the OECD adopted a set of voluntary 'Guidelines for Consumer Protection in the Context of Electronic Commerce'⁶⁴ to assist in developing consumer protection mechanisms for electronic commerce transactions. In 2009, the OECD launched a review of these Guidelines to respond to new and evolving challenges in the internet economy.
- 7.12 Under the review process, in December 2009, the OECD's Committee on Consumer Policy held a conference on Empowering E-Consumers: Strengthening Consumer Protection in the Internet Economy.⁶⁵ The conference addressed a number of issues including consumer challenges in online and mobile payments. Stakeholders notably

⁶⁴ www.oecd.org/document/51/0,3343,en_21571361_43348316_1824435_1_1_1_1,00.html

⁶⁵ www.oecd.org/dataoecd/32/10/45061590.pdf

acknowledged that, although progress has been made in developing a vast array of payment mechanisms, price and payments are a source of a significant number of consumer complaints.

- 7.13 As regards payment security, the conference also noted that industry has been involved in producing solutions, through voluntary codes and best practices. For example, to prevent information interception during the transmission of credit card information, secure socket layer (SSL) service is commonly used.⁶⁶ Additional systems have also been developed, such as MasterCard SecureCode and 'Verified by Visa', both of which protect cards with a password, created by the user, which assures that only they can use the card to make online purchases.
- 7.14 The OECD is now looking into online and mobile payments in more detail. A draft report is being developed to explore market developments and identify related consumer issues. Policy guidance will then be developed through 2012, building on both the findings and conclusions in the report and on discussion at an expert meeting, to be held at the OECD in Paris on 14 April 2011. The work will help determine and identify any need to amend the 1999 Guidelines in this area. The OFT will consider any relevant findings and outcomes of this prospective project.
- 7.15 The OFT will use consumer campaigns to highlight the various redress options attached to specific payment mechanisms and educate consumers about the ways in which they can transact online more safely. We will signpost consumers to 'Get Safe Online' to allow them to find up-to-date information on how to keep themselves safe on the internet.

⁶⁶ SSL description: Encryption and decryption allows the secure transfer of information between an internet browser and server (that is the buyer and seller). This data cannot be intercepted or changed during transmission.

Improve transparency and security of transactions: Initiatives	Lead agency, key partners
PRIORITY 7.iii Work with credit card companies and other online payment providers to promote safe payment practices. The OFT to consider any relevant findings from OECD work.	OFT and Industry
7iv Continue work on improving transaction transparency (for instance from Advertising of Pricing Study and related work).	OFT, TSS and other regulators who can enforce CPRs

Leverage learning and redress

- 7.16 Part of the 'Just Tick It' scam ticketing campaign in July 2010 encouraged consumers to check the legitimacy of a website before spending any money. This included tips on finding out what others are saying about a website, checking the geographical address and landline number of the company selling the tickets and ensuring the company can provide ticket details. All of these tips are applicable more widely to any online purchase.
- 7.17 The OFT will continue with messages from the 'Just Tick It' campaign to encourage consumers to make greater use of the tools available to them to buy and sell safely online.
- 7.18 As mentioned previously (Enforcement section, paragraph 5.27), in October 2010, the OFT assisted the FTC with an investigation into a US company selling to UK consumers. The OFT wrote to UK consumers that complained to the OFT or the FTC to advise them of

their chargeback rights in relation to goods purchased from websites operated by this US company.⁶⁷

- 7.19 In April 2011 a pilot will begin to test new powers under the Regulatory Enforcement and Sanctions Act 2008 (the RES Act). This Act provides a framework for regulators to be granted access to a range of civil sanctions as an alternative to criminal offences. The OFT expects to be part of this pilot along with 14/15 TSS. The OFT will also be working with BIS and LBRO to deliver guidelines on how this pilot might operate.
- 7.20 In May 2010, the OFT carried out a project to look at the strengths and weaknesses of the UK consumer redress landscape,⁶⁸ which has given a clearer picture of the distribution of ADR mechanisms in the UK. The project found that consumers appear better covered in relation to services than goods and that the provision of ADR has improved in some sectors over recent years.
- 7.21 One of the main barriers to using ADR schemes is a lack of awareness that such schemes exist. The Consumer Direct website has details on the different mechanisms available and also provides a link to the European Consumer Centres network (ECC-Net)⁶⁹ which can facilitate access to ADR schemes in participating countries.
- 7.22 Problems with cross-border transactions can add a layer of confusion about where consumers should seek advice. ICPEN⁷⁰ has recently launched a new website to try to address this. The website provides consumers with information on avoiding scams, and how to shop

⁶⁷ www.oft.gov.uk/OFTwork/consumer-enforcement/internet-enforcement/chargebackletter/

⁶⁸ www.oft.gov.uk/OFTwork/policy/mapping-uk-consumer-redress

⁶⁹ www.ukecc.net/default.asp

⁷⁰ ICPEN is a forum of consumer protection authorities that encourages global co-operation aimed at reducing fraudulent, deceptive and unfair trading practices around the world.

safely online. It also includes information on how to lodge a complaint and where to look for help.⁷¹

7.23 The OFT will continue to monitor on-going developments within the EU and will use campaigns to encourage consumers to make more use of the tools available to them to buy and sell safely online and to promote awareness of the various redress options they have when things go wrong.

Leverage learning and redress: Initiatives	Lead agency, key partners
PRIORITY 7.v Investigate development of an online reporting system for consumer problems. ⁷²	OFT
7.vi Continue to monitor progress on redress at EU level, continue work on redress and ADR where priorities allow.	OFT and BIS
PRIORITY 7.vii Take enforcement action to help consumer redress, facilitate charge-backs (for example, the Civil Sanctions Pilot).	OFT, TSS
7.viii Promote consumer learning, information sharing, and effective use of consumer reviews (see business compliance, paragraph 6.15).	OFT and Industry, Citizen's Advice, Which? Consumer Focus and other relevant consumer bodies

⁷¹ www.icpen.org/for-consumers/do-you-have-a-crossborder-dispute

⁷² It is envisaged that this system will also be used for the reporting of competition issues. To avoid duplication with Action Fraud, consumer complaints which fulfil certain criteria are likely to be referred to Action Fraud to enable them to collect the additional information.

8 NEXT STEPS

- 8.1 The majority of recommendations from the strategy for protecting consumers online fall within the remit of the OFT. These recommendations have been prioritised within existing workstreams and are underway or are included in forward plans. They are discussed in more detail in the table below, which outlines progress to date, and proposed next steps.
- 8.2 Two recommendations, which fall outside the OFT's remit, are likely to require additional funding to enable them to proceed as described in the strategy. These recommendations are also likely to be affected by the review of the consumer landscape. A public consultation on the desirability of moving all relevant Central Government funding for consumer bodies towards Citizens Advice and TSS will take place in early 2011. The OFT intends to feed into the consultation.
- 8.3 The key recommendations that fall outside the current remit of the OFT are:
- improving intelligence: developing a UK wide e-consumer protection intelligence system (possibly using IMD), and building a national intelligence capability, leveraging and supporting the existing Regional Intelligence network and Regional Intelligence Units (RIUs)
 - developing a small number of dedicated, expert teams within TSS to provide UK-wide internet coverage.
- 8.4 Where the OFT is able to assist with progressing and supporting these recommendations, it will continue to do so.

Monitoring Progress

- 8.5 Monitoring and evaluating the activities we undertake as part of protecting consumers online will help to assess the effectiveness and efficiency of interventions. This understanding will ensure that interventions are well developed, targeted and provide value for money. In addition, monitoring the outcomes will enable us to refine

and improve initiatives which do not appear to be delivering the required benefits.

8.6 We recognise that monitoring and evaluating the impact of the strategy will not be easy, as there are many other contributory factors which will impact business compliance, capability in internet enforcement, and consumer confidence. These include:

- Initiatives to build internet capability across the UK, for instance the continued roll-out of the internet project undertaken by SELT,⁷³ work and investment undertaken by Local Authorities, partnership working between TSS, OFT and other internet enforcers and improved dissemination of intelligence from NFIB and others.
- Businesses themselves becoming more familiar with the relatively new body of consumer protection regulation, and the on-going development of BusinessLink and ERWIN helping to improve awareness. Moreover business compliance could also increase as a result of actions by third parties, for example platforms such as Amazon and eBay, to reinforce consumer protection regulations through their terms and conditions of operation.
- Increasing consumer confidence over time as consumers become more skilled and familiar with the internet,⁷⁴ as the underlying demographic mix changes, and as companies refine their consumer protection offerings. A number of other initiatives (such as Race

⁷³ SELT is a partnership formed to tackle scams across the East of England, London and the South East, covering 61 local authority Trading Standards services, and a total population of 18 million people. It consists of the Scambusters, East of England Trading Standards Association, London Trading Standards Association & Trading Standards South East Ltd (SELT).

⁷⁴ See also 'Perceptions of Security and Risks on the Internet, Experience and learned levels of trust', 24 January 2008 (Tentative conclusions: Experts learn how to deal with online risks; skills will diminish level of importance of risks. Internet literacy and exposure to the internet will increase people's levels of trust.)

Online 2012's Manifesto for a Networked nation) should also increase consumer confidence and participation online.

- 8.7 However, it is possible to identify indicators which we believe would help us gain a better understanding of the impact of the strategy. In particular, it will be possible to gauge progress and impact of specific initiatives, outlined below.

Internet effectiveness

- 8.8 Two recent pieces of research, one undertaken by the OFT,⁷⁵ and a second one carried out by the BIS funded project run by SELT on Internet Enforcement⁷⁶ have established baselines for different aspects of internet effectiveness. Both organisations plan on repeating the surveys, with their results potentially informing our monitoring of progress on the supply side of enforcement capacity.
- 8.9 The OFT study is a simple self-assessed measure of the level of capability across the TSS network with 67 per cent of TSS responding (see diagram 2, 'Internet Enforcement Capability across the TSS Network, November 2010'). We intend to repeat this questionnaire on an annual basis to understand how internet enforcement capability is developing on the supply side.
- 8.10 The SELT baseline is more comprehensive, and covers the period 1 April 2009 to 31 March 2010, with responses from 79 per cent of TSS. At the start of the project, 47 per cent of TSS had a stand-alone internet investigations computer, approximately 10 per cent of local authority

⁷⁵ Internet Effectiveness across the TSS Network, Self-assessed capability based on a questionnaire sent to all TSS, November 2010, response rate 67 per cent, total responses 131

⁷⁶ E-Consumer Protection Project 'Trading Standards e-consumer protection and internet enforcement Project', Restricted Document. BIS have provided funding for a three year initiative which will enable trading standards to deliver a national project on the area of e-consumer protection and internet enforcement. It is being managed in partnership by the East of England, London and South East Trading Standards (SELT) authorities.

officers had received formal training on internet investigations, 71 per cent of TSS had undertaken compliance work regarding internet activity, and 47 per cent had undertaken internet test purchases. The SELT project plans to ask for questionnaire returns on a six monthly basis to inform the project.

- 8.11 Understanding the need for intervention involves measuring the number of problems facing consumers and understanding how this changes over time. This could be aided by additional by an additional survey (which could be done through something like the British Crime Survey), the percentage of these problems that are reported (use the same source), and the percentage of those that are addressed by the OFT and TSS.
- 8.12 However, other existing proxies are useful in terms of indicating progress and general experience of users. For instance, the Oxford Internet Institute (OII) carries out a biannual survey of internet users,⁷⁷ and asks if they have 'bought something which has been misrepresented on a website'. Similarly, the OFT commissioned a survey by FDS⁷⁸ which also investigated consumers experiences online.
- 8.13 Monitoring the intelligence-led and coordinated approach recommended by the strategy will involve:
- monitoring the systems and processes to support an effective intelligence function, for example the percentage of investigating officers with direct access to input into an intelligence system, the use of standardised intelligence systems in common use for internet enforcement and the percentage of investigating officers with intelligence training

⁷⁷ The most recent Oxford Internet Survey (OxIS) is 'The Internet in Britain 2009', <http://microsites.oii.ox.ac.uk/oxis/>

⁷⁸ Attitudes to Online Markets (OFT1253), FDS, August 2010. www.of.gov.uk/shared_of/consultations/eprotection/oft1253

- monitoring the extent, breadth and relevance of intelligence and shared intelligence sources, for example the number of UK enforcement agencies able to use OFT/TSS intelligence directly or through ad hoc processes (automated systems and information sharing MoUs), the number of country databases capable of being searched by UK enforcers or other approximate measures of global coverage
- monitoring the effect or outcome of good intelligence use and coordination, for example an assessment based on qualitative and quantitative data. Quantitative analysis might consider the time taken to ascertain enforcement responsibilities, the use of tasking systems (and percentage of TSS/OFT units covered). Qualitative analysis might include interviews with investigating officers and other relevant stakeholders.

Business compliance

8.14 Measuring the business compliance actions of this strategy will include:

- monitoring and evaluating the use and effectiveness of the new OFT web site containing guidance for businesses and consumers on DSRs, and
- monitoring levels of compliance with DSRs and other consumer protection regulations as measured by.

Consumer confidence in online markets

8.15 A number of the actions outlined in the empowering consumers section of the strategy focus on consumers' awareness of their online rights and where they can go for assistance. BIS has historically undertaken surveys to assess consumer awareness of both of these aspects. In addition, research has been conducted on behalf of the OFT (for example the Attitudes to Online Markets Survey, and research for

market studies such as Internet Shopping⁷⁹ and Online Targeting of Advertising and Prices⁸⁰). It is hoped that these or similar can be undertaken in the future.

- 8.16 More widely, there is a range of more general surveys, including consumers' attitudes to enforcement, redress and confidence. Examples of such include the Oll surveys (covering consumer attitudes to security, trust, and confidence on the internet) the EC's Consumer Markets Scoreboard (containing information on consumers trust in sellers, (see diagram 1, page 10), national polling data, and the Organisation for Economic Co-operation and Development (OECD) data. Lastly, government bodies such as the ONS, BIS and the OFT have analysed consumers use of and trust in online markets.
- 8.17 Where relevant, we will use such survey results above to monitor changes and use this to inform our approach. In addition we will monitor the work of the OECD Working Party on Indicators for the Information Society.

⁷⁹ www.offt.gov.uk/shared_offt/reports/consumer_protection/oft921.pdf

⁸⁰ www.offt.gov.uk/shared_offt/business_leaflets/659703/OFT1231.pdf

Key Recommendations within current planning

5. Developing More Effective Enforcement (Improving data-sharing and intelligence)

Reference	Initiative	Status	Next Steps
5.i	Improve data-sharing and intelligence between and amongst the OFT and TSS by developing an e-intelligence system (possibly using IMD ⁸¹) and building national intelligence capability (including leveraging and supporting the RIO network).	<ul style="list-style-type: none">• Will require additional funding.	<ul style="list-style-type: none">• Dependent on funding.

⁸¹ IMD – Intelligence Management Database (currently used by all Regional Intelligence Officers across the UK, the OFT and around 35 per cent of TSS).

Reference	Initiative	Status	Next Steps
5.ii	Contribute to national data-sharing, working with NFIB and other agencies to share intelligence and Consumer Direct data.	<ul style="list-style-type: none"> • Manual data exchange with NFIB currently on manual ad hoc basis. • MoUs with other key enforcers (Police, Ofcom, SOCA, HMRC, etc), in place. • OFT in discussions with NFIB over sharing data from NFIB. • Web links on CD sign-posting Action Fraud. 	<ul style="list-style-type: none"> • Move to automatic data exchange with NFIB.
5.iii	Work towards sharing consumer complaints data globally for example via Consumer Sentinel. ⁸²	<ul style="list-style-type: none"> • OFT seeking legal advice on legislative constraints. • Discussions underway with Consumer Sentinel. • OFT progressing data-sharing across the CPC network. 	<ul style="list-style-type: none"> • Use legal advice to determine course of action. • Include data where possible on future CPC portal (2011).

⁸² Consumer Sentinel provides law enforcement members with access to consumer complaints provided directly to the U.S. Federal Trade Commission by consumers, as well as providing members with access to complaints shared by data contributors.

5. Developing More Effective Enforcement (Developing internet enforcement capability)

Reference	Initiative	Status	Next Steps
5.iv	Build web portal for TSS & CPC networks to enable capability sharing and coordination. Migrate enforcement tools (such as manuals and pro-forma letters) to portal.	<ul style="list-style-type: none"> • OFT seeking funding from the European Commission's Executive Agency for Health and Consumers (EAHC) to develop web site for CPC network, and share know-how. • OFT is investigating feasibility of building in-house a portal for OFT and TSS, and sharing this work with the CPC network. • Enforcement manual complete. 	<ul style="list-style-type: none"> • Develop CPC Portal, and populate with data, enforcement tools, etc (2011). • Hold workshops (2011-2012). • Get project approval for UK portal, develop UK portal (2011).
5.v	Work with TSS and other key players to develop a small number of dedicated, expert teams, within TSS to develop UK wide Level 2 coverage. Invest in critical infrastructure for key TSS and the OFT.	<ul style="list-style-type: none"> • Will require additional funding. 	<ul style="list-style-type: none"> • Dependent on funding.

Reference	Initiative	Status	Next Steps
5.vi	Take strategic enforcement action to clarify UK internet case law (including key issues such as intermediary liability, redress for consumers, the legal status of digital products and the application of the CPRs to emerging trading practices) to ensure internet markets function effectively and TSS can leverage legal action.	<ul style="list-style-type: none"> • Recent cases include: <ul style="list-style-type: none"> ○ redress– Unfair trading by online electronics retailer (Undertakings obtained to refund the affected consumers and ensure that future orders are delivered on time). Also, OFT facilitates charge backs for UK consumers in context of FTC investigation ○ CPRs – European Health Insurance Cards ○ working with TSS to leverage legal action – current focus deceptive online selling of government services. 	<ul style="list-style-type: none"> • On-going work, driven by intelligence and internal prioritisation.
5.vii	Work with Nominet to improve awareness of, and ability to respond to, abuses using .uk domain names.	<ul style="list-style-type: none"> • Initial scoping work begun. • Nominet currently consulting with stakeholders on 'Dealing with domain names used in connection with criminal activity'. 	<ul style="list-style-type: none"> • Nominet and OFT to work on options to improve awareness and reduce abuse beginning 2011.

5. Developing More Effective Enforcement (Coordinate enforcement action)

Reference	Initiative	Status	Next Steps
5.viii	Use the web portal (see 5.iv) as a site for coordinating enforcement action.	<ul style="list-style-type: none"> • Currently coordination is facilitated through TS Interlink. 	<ul style="list-style-type: none"> • Get project approval for UK portal, develop UK portal (2011).
5.ix	Clarify remits of OFT and TSS, develop links and informal coordination mechanisms with other law enforcement agencies.	<ul style="list-style-type: none"> • Remit of the OFT e-consumer protection is in protecting the economic interests of consumers online. The majority of OFT's online enforcement deals with civil breaches of consumer protection legislation. 	<ul style="list-style-type: none"> • On-going liaison with other enforcers.
5.x	Further develop national and international coordination function, liaising with national and international regulators and enforcers.	<ul style="list-style-type: none"> • Preliminary work undertaken on increasing the capability of the CPC network. • Participation with ICPEN, OECD and CPC, staff secondments with FTC, etc. 	<ul style="list-style-type: none"> • Continuing participation with CPC and ICPEN. • OFT is progressing the development of the ICPEN country directory of regulators and enforcers (2011).

6. Promoting Business Compliance (Inform business)

Reference	Initiative	Status	Next Steps
6.i	Continue to improve guidance and sign-posting for businesses to ensure they have access to clear, relevant information - leveraging Business Link and initiatives such as the SOGA Hub.	<ul style="list-style-type: none"> • SOGA hub launched in September 2010. The hub is currently being publicised to business and being evaluated. • Advice on the DSRs is being developed for businesses. 	<ul style="list-style-type: none"> • Develop and roll-out of DSRs information for businesses (March 2011). • Content available for business on the OFT website made available on, or accessible from, the Business Link website (January 2011). • Review of all OFT website content to ensure content is user friendly, relevant for the target audience, accessible and optimised for the web.
6.ii	Continue to check for compliance, inform non-compliant businesses and direct to guidance materials.	<ul style="list-style-type: none"> • OFT active in EU-coordinated web sweeps, for example into ticketing websites and online marketing and advertising to children and young adults in 2010. 	<ul style="list-style-type: none"> • Continue active role in EU-coordinated web sweeps and take follow up action where appropriate.

6. Promoting Business Compliance (Cooperate with business)

Reference	Initiative	Status	Next Steps
6.iii	<p>Work with industry to ensure that:</p> <ul style="list-style-type: none"> • Website designers are provided with information which helps them to build compliance into the websites they produce for online retailers. • The utility of consumer feedback mechanisms is reinforced. 	<ul style="list-style-type: none"> • Potential problems relating to online consumer-generated feedback being monitored with a view to targeted enforcement action where appropriate. 	<ul style="list-style-type: none"> • Website designers alerted to the new DSRs guidance (see 6.i above) once rolled-out. • Continue to monitor issues relating to online consumer-generated feedback and to take targeted action where appropriate.
6.iv	<p>Initiate and maintain channels for ongoing dialogue with industry for the purposes of horizon scanning, intelligence sharing and problem solving.</p>	<ul style="list-style-type: none"> • OFT's internet enforcement team has begun to initiate and develop effective communication channels with key internet platforms to ensure that the OFT has timely access to relevant info. regarding trader accounts where there is evidence of consumer detriment. 	<ul style="list-style-type: none"> • Communication channels with online platforms developed and maintained. • Know-how workshop held with other EU consumer protection authorities to share best practice (autumn 2011).

7. Empower consumers (Educate consumers)

Reference	Initiative	Status	Next Steps
7.i	Work with other organisations including government departments and consumer bodies to ensure that we are consistent in the messages we give consumers about online markets. Plan communications to avoid duplication, enable maximum reach.	<ul style="list-style-type: none"> • Feedback from initial workshop and consultation responses indicates agreement from other organisations with this initiative. • Workshop with a group of consumer agencies in October 2010 explored common messaging. All in attendance saw the need for consistent messaging and sharing of plans, but identified that using identical key campaign messages could be difficult. 	<ul style="list-style-type: none"> • Partnership with other consumer facing organisations to ensure we provide consistent messages on buying and selling online to focus top tips. • Investigate low cost consumer education channels.
7.ii	Develop education messages focusing on consumer rights when buying online. Disseminate messages through a range of channels.	<ul style="list-style-type: none"> • Scams Awareness Month's and the 'Just Ticket' scam campaigns both currently provide tips on buying and selling online. 	<ul style="list-style-type: none"> • The OFT will develop educational messages to focus on informing consumers of their rights when shopping online.

7. Empower consumers (Improve transparency and security of transactions)

Reference	Initiative	Status	Next Steps
7.iii	Work with credit card companies and other online payment providers to promote safe payment practices. The OFT to consider any relevant findings from OECD work.	<ul style="list-style-type: none"> • Work currently ongoing at OECD to consider whether there is a need for a policy paper or to amend current guidelines. 	<ul style="list-style-type: none"> • The OFT will use consumer campaigns to highlight the redress options and educate consumers about the ways in which they can transact online more safely.
7.iv	Continue work on improving transaction transparency (for instance from Advertising of Pricing Study and related work).	<ul style="list-style-type: none"> • During the current market study, the OFT is looking to clarify and update the understanding of consumer harm that arises from potentially misleading advertising and pricing. 	<ul style="list-style-type: none"> • The OFT will actively monitor price promotions and, where necessary, will take targeted national enforcement action against firms using practices that constitute serious breaches of the law.

7. Empower consumers (Leverage learning and redress)

Reference	Initiative	Status	Next Steps
7.v	Investigate development of an online reporting system for consumer problems. ⁸³	<ul style="list-style-type: none"> Initial scoping exercise in progress. 	<ul style="list-style-type: none"> Dependant on scoping exercise and available resources.
7.vi	Continue to monitor progress on redress at EU level, work on redress and ADR where priorities allow.	<ul style="list-style-type: none"> The OFT carried out a project to look at the strengths and weaknesses of the UK consumer redress landscape. 	<ul style="list-style-type: none"> Ad hoc monitoring of consumer redress.
7.vii	Take enforcement action to help consumer redress, facilitate charge-backs.	<ul style="list-style-type: none"> The OFT wrote to consumers advising them of their chargeback rights in October 2010 (see paragraph 7.18). 	<ul style="list-style-type: none"> Continue to take enforcement action where appropriate.
7.viii	Promote customer learning, information sharing, and effective use of consumer reviews.	<ul style="list-style-type: none"> Potential problems relating to online consumer-generated feedback being monitored with a view to targeted enforcement action where appropriate. 	<ul style="list-style-type: none"> Continue to monitor issues relating to online consumer-generated feedback and to take targeted action where appropriate.

⁸³ It is envisaged that this system will also be used for the reporting of competition issues. To avoid duplication with Action Fraud, consumer complaints which fulfil certain criteria are likely to be referred to Action Fraud to enable them to collect the additional information.

A RESPONSES TO CONSULTATION

- A.1 The public consultation on the strategy for protecting consumers online was launched on the 23 July and closed on the 13 October 2010. Copies of the consultation document were available on the OFT website. In addition, interested organisations and individuals received a link to the consultation document by email. Other parties helped to alert a wider audience: the consultation was highlighted in blogs (for example, moneysaver) and in various newsletters and emails (BISs newsletter, IMRG, TSS, BRC, Nominet). To compliment the approach above, the team held a number of workshops and interviews on various aspects of the consultation.
- A.2 The OFT received 45 written responses. The OFT is very grateful for all of the responses to this consultation and has considered all of the comments and suggestions made. A summary of the responses to the strategy for protecting consumers online is contained within a separate document on the OFT website.

B LEVELS OF E-CONSUMER INTERNET ENFORCEMENT

Level	Skills Required	Types of Cases
Level 0	Addressing internet complaints with civil advice only.	<ul style="list-style-type: none"> N/A
Level 1 <ul style="list-style-type: none"> Low complexity. Medium detriment. 	<ul style="list-style-type: none"> Check website compliance/perform targeted websweeps. Basic evidence gathering Domain name/IP address owners search – whois, IANA, Samspace etc. Test purchases/browsing with stand alone/ anonymous computer. 	<ul style="list-style-type: none"> UK based (local) – standard investigation. Local trader. Online auction/platform seller failing to deliver goods. Technical/minor/ inadvertent breaches.
Level 1-2 Depending on ISP response <ul style="list-style-type: none"> Low/med complexity. Med/high detriment. 	<ul style="list-style-type: none"> Notice and take down. Search and seizure. 	<ul style="list-style-type: none"> UK based (local/ regional/national) – standard investigation.
Level 2 <ul style="list-style-type: none"> Medium complexity. High detriment. 	<ul style="list-style-type: none"> Test purchases with stand alone/anonymous computer Forensic intelligence. gathering using standard forensic software packages for example, AccessData’s Forensics Tool Kit. Video/screen capture software for example, Cam studio. 	<ul style="list-style-type: none"> UK based (regional/national) – (non) standard investigation. Negligent, flagrant, deliberate, multiple breaches.
Level 3 <ul style="list-style-type: none"> High complexity. Very high detriment. 	<ul style="list-style-type: none"> Liaising with overseas enforcers. Complex forensic intelligence gathering. Analysis of rapidly evolving sites for example, Websence, Brightcloud. Sniffer/debugger software. Tools to analyse imaged. data for example, to recover deleted data/crack encryption. 	<ul style="list-style-type: none"> National/Cross border cases. Precedent setting. Fraudulent/(serious) organised crime.

C GLOSSARY OF TERMS

List of terms used in the strategy

Term	Definition
ACCC	Australian Competition and Consumer Commission
ACPO	Association of Chief Police Officers
ACTSO	Association of Chief Trading Standards Officers
ADR	Alternative Dispute Resolution
BIS	Department of Business, Innovation and Skills
CESG	The National Technical Authority for Information Assurance
CPC	Consumer Protection Cooperation
CPNI	Centre for the Protection of National Infrastructure
CSOC	Cyber Security Operations Centre
DSR	Consumer Protection (Distance Selling) Regulations 2000
EAHC	European Commission's Executive Agency for Health and Consumers
EC	European Commission
ECC-Net	European Consumer Centres Network
EHIC	European Health Insurance Card
ERWIN	Everything Regulation, Whenever It's Needed
FSA	Financial Services Authority

FTC	Federal Trade Commission
GCHQ	Government Communications Headquarters
HMRC	HM Revenue and Customs
ICPEN	International Consumer Protection and Enforcement Network
ICO	Information Commissioners Office
IMD	Intelligence Management Database
IMRG	Interactive Media in Retail Group
ISP	Internet Service Provider
LA	Local Authority
LAP	London Action Plan
LG Reg	Local Government Regulation
LILO	Local Intelligence Liaison Officer
MoD	Ministry of Defence
MoJ	Ministry of Justice
MoU	Memorandum of Understanding
NFIB	National Fraud Intelligence Bureau
OCSIA	Office of Cyber Security and Information Assurance
OECD	Organisation for Economic Cooperation and Development
OFT	Office of Fair Trading
PCeU	Police Central e-crime Unit

RIO	Regional Intelligence Officers
SELT	Scambusters, East of England Trading Standards Association, London Trading Standards Association & Trading Standards South East Ltd.
SME	Small and Medium Enterprises
SOCA	Serious Organised Crime Agency
SOGA	Sale of Goods Act Hub
SSL	Secure Socket Layer
TSI	Trading Standards Institute
TSNW	Trading Standards North West
TSS	Local Authority Trading Standards Service