



OFT consultation on E-Consumer Protection

Response from Citizens Advice and Citizens Advice Scotland

October 2010

Introduction

The Citizens Advice service provides free, independent, confidential and impartial advice to everyone, about their rights and responsibilities. It values diversity, promotes equality and challenges discrimination. The service aims:

- to provide the advice people need for the problems they face; and
- to improve the policies and practices that affect people's lives.

The Citizens Advice service is the largest independent network of free advice centres in Europe, providing advice from over 3,000 outlets, including GPs' surgeries, hospitals, community centres, county courts and magistrates' courts, throughout Wales, England and Northern Ireland. In addition, over 80 bureaux provide advice through over 200 service points in Scotland.

Citizens Advice Scotland (CAS) is the umbrella organisation for Scotland's network of over 80 Citizens Advice Bureau (CAB) offices. These bureaux deliver frontline advice services through more than 200 service points across the country, from the city centres of Glasgow and Edinburgh to the Highlands, Islands and rural Borders communities.

Citizens Advice Bureaux in England and Wales assisted two million clients with over seven million problems in 2009/10, including 6,200 about private sales and internet auctions. The Citizens Advice service in Scotland dealt with over 500,000 new issues in 2009/10, representing around 1,500 for every day of the year and a nine per cent increase from the year before. 16,953 of these were new consumer issues and over 700 were in relation to private sales and internet auctions.

General comments

Access to shopping on line provides huge opportunities for those with internet access. We are, however, very concerned about the opportunity for fraud that the internet provides and the speed with which opportunities for scams and frauds are taken up. For example, scams were targeted at people with potential tax underpayments as soon as news of the tax problem was made public. This happens in all mediums but the internet provides speed and anonymity. Being able to find problem traders and fraudsters must be key to any strategy for e-consumer protection, if the objective of increased levels of sustainable trust and a UK position of global leadership in online enforcement are to be met.

Citizens Advice and Citizens Advice Scotland support the need for an e-consumer protection strategy. We particularly welcome the proposal in this consultation to address the need for:

- sustainable consumer confidence that empowers consumers and takes particular account of the most vulnerable;
- effective responses to change; and
- improving effective enforcement, including the promotion of business compliance and a focus on use of resources.

To achieve this, regulators and enforcers, businesses who trade fairly and consumers must all be active participants. The consultation suggests that the OFT works with business, however it should be working with consumers at the same time.

A joined up approach must include:

- The use of existing reporting tools to enable consumers to report frauds and scams. Action Fraud is the single reporting portal for frauds where people have lost money but they do not yet use the intelligence consumers and advisers can provide when a fraud first appears but before money has been lost.
- Consumers should be able to access information about companies breaching consumer protection law as soon as regulators and enforcers first see a problem rather than at the end of the enforcement process. Markets and consumers can then be alerted to good and bad practices quickly, before huge numbers of consumers are affected and before the practice becomes widespread.
- We strongly support pre-payment protection and are pleased to note its inclusion in this consultation. To enable consumers to have confidence buying online we suggest the use of escrows and the Scottish equivalent where consumers' pre-payments can be ring fenced.
- Improving the traceability of businesses selling over the internet. Although there is EU and UK legislation requiring businesses to identify themselves, CAB clients often report that they cannot locate businesses that they bought from over the internet when things go wrong, often because the web site is no longer accessible, as in the cases in the section below show.
- Engaging internet service providers used by business, so that they react quickly to enforcers who inform them of illegal trading practices.

This should help enforcers concentrate their capacity on those traders who do most harm.

CAB case examples

This section includes a few examples of the many cases reported by bureaux in relation to buying goods and services online.

Several of the cases below illustrate a range of issues where consumers are experiencing problems. We have used headings as a guide to the main issue raised.

Rogue trading

A Hertfordshire CAB client was held by the police for being in possession of a stolen car, which he had had no trouble registering with DVLA. He had also successfully registered a change to personalise number plates. He had found the car for sale on the internet, through a well known magazine, and had paid £11,000 to a man who claimed to be a dealer working from home.

A CAB client from Essex had used their online payment account to accept payment for a scooter they were selling. Several months later, the online payment facility business claimed the buyer had used a credit card fraudulently and took the payment back from the client's account. As the client had left positive feedback he wanted to change it. The internet auction web site used refused to allow this because of the time lapse.

A Hampshire CAB client found a blog that explained why they had only received one of three pairs of power stilts they had bought online. Following several excuses from the trader, including some threatening messages, the client discovered that the stilts were illegal in England. On the blog the seller had blamed meddling kids for foiling his plans for a good money making scheme. The online payment facility refused to refund the money on the grounds that the client had received one of the three pairs.

Cross-border online purchases

A West of Scotland CAB client who teaches English overseas had signed up to start a teaching position with a school based in France, having communicated with the Principal and the school's Director by email. She had sent scanned documentation including passport details and a deposit for her accommodation. She sought advice when she was told that she had been the victim of a computer scam and nothing could be done for her.

An East of Scotland CAB reported that a client from Austria had been left with a faulty hire car having hired from a car hire firm through the internet. The car was delivered to the client without petrol and paid for in cash. No receipt was given. When the car started breaking down the client contacted the company and found they could not get through. They had no option but to abandon the car they had paid £1,000 to use.

Online prices

A West of Scotland CAB reported a client who had purchased a dress from an upmarket boutique on the basis that it was being sold for half the original £700 price. She had then bartered and agreed a price of £250.00. When she looked on the internet for another item she noticed that the same dress was advertised at £235.00 but was being sold for under that price. The shop would give a credit note but not a refund.

Payment protection

CAB clients from North London bought a trailer on an internet auction site but found that the online payment facility, which claimed to offer a mediation service, closed access to this provision when the seller had not responded in seven days. The advertisement was misleading, misrepresenting the condition of the trailer, and the seller had insisted on being paid the £1,803 in cash. The client found later that it needed £1,400 worth of work to make it fit for purpose.

A West of Scotland CAB client bought goods on the internet from a.co.uk web site and paid using the payment system operated with an online auction site. The client got suspicious when they did not receive a confirmation email for the purchase. The goods are faulty and the client has discovered that the person who runs the web

site from China is a convicted internet fraud criminal. The pre-payment protection scheme would not help as the web site was not run through their parent internet auction site.

A CAB client from Devon thought they had pre-payment protection with a payment scheme that claimed to provide cover for faulty goods for all internet purchases. But when they tried to claim, they found that the 'buyer complaint policy' only covered purchases made on their sister online auction site.

An unemployed CAB client from South-East Wales had bought a sofa on an internet auction web site for £350. They accepted the trader's explanation that there was a manufacturing delay but after a month was notified the trader had gone bust. Having paid via a popular online payment scheme, the client thought his money was safe, only to find that their 'buyer protection policy' only provided cover for the first 45 days from purchase.

Failure to deliver consumer rights

A West of Scotland CAB client bought a kitchen for £1,500 from a company trading on the internet. The client had no receipt or other paperwork for the purchase. The kitchen arrived damaged and only partially complete. The client sought advice after they had complained several times and been promised a replacement that never arrived.

A CAB client from Berkshire told the bureau she thought the company who failed to deliver the goods she bought and then failed to send a refund were counting on customers feeling that it was not worth the trouble of taking a court case. She had paid £90 for a present intended for her grandson and was told first that they were out of stock, then that the item had been sent. The courier had no record of the item and eventually her online account showed a reimbursement. The company claimed a cheque had been sent but no cheque arrived. By this time the protection she had sought by using an online payment scheme said it was too late to intervene on her behalf. When she checked she found feedback from others in the same position. She had told her local Trading Standards and planned to take the case to court.

A North of Scotland CAB client found that a different sum had been taken on her credit card than the price stated when she ordered the item via the internet. She had tried to return the item as instructed on two occasions but the seller failed to collect the goods. The client then received threatening e-mails from the firm stating that they will report her for fraud. Trading Standards suggested that she go to the bureau.

An East of Scotland CAB reports of a client who bought two medical products on the internet at a cost of £11.99 each but was then charged more than £60 for each on her bank statement. A "pop up" had advertised the medical slimming product at the special introductory price of £11.95. The client purchased this product but in May and June two further deductions were made from her current account. The company say she had accepted the promotional/introductory offer and then not cancelled it and their terms include continuing supply at the full price. The client

does not have a copy of the agreement and she has since set up a new PC and feels she is unlikely to be able to trace the web site.

A North of Scotland CAB client ordered a pool table from an online dealer which was advertised at £495 and clearly stipulated "free delivery within the UK". The seller contacted the client by email stating that there was a discrepancy between his credit card details and his address and at the same time told him they would not deliver to the Island where he lives. The client asked if they would deliver the table to the next big city and was told that they would deliver only if client paid £661.

A CAB client from Greater Manchester discovered that whilst the high street retailer from whom she had bought a DVD player acknowledged the fault she was experiencing on their website, they had failed to withdraw the item from sale.

Contact problems

A West of Scotland CAB client bought boots on the internet. They took too long to arrive and the client tried to cancel using the cancellation system advertised but there was no answer on the phone and no means to leave messages. The client's emails were ignored. When the boots finally arrived they were immediately returned to the seller. The client has heard nothing from the company despite repeated attempts to contact them by mail, email and phone.

Credit regulation

A South of Scotland CAB reported the case of a debt client who was approved for a £4,000 loan online with interest rates of over 40%. This company features in negative feedback and appears to be giving credit to people with a poor credit history and requiring someone to act as guarantor. The company pursues the guarantor if the debtor fails to make repayments.

An East of Scotland CAB client was in the process of applying online for a loan with a loan company and filled in his phone number. Soon after, and while he was still filling out the form the client received a call from the loan company asking for his personal and bank account details. The client did not want the loan yet and made it clear that they did not want the loan processed at this stage. The company ignored this and both processed the loan immediately and withdrew a processing fee from the client's account. The client feels he was scammed.

A CAB client from Gloucestershire in receipt of benefits decided not to complete the online application she had begun for a loan. She had already given her bank details and found that two payments of £70 had been taken from her account for what was claimed to be 'administrative charges'.

Copyright

A Tyne and Wear CAB reported that their client's wife had received paperwork claiming she had illegally downloaded a film. A High Court order was included which the wife had misinterpreted as a court order for her to pay the £495 demanded. Although the woman was sure she had not downloaded the film, she planned to pay. The client sought advice when he discovered the solicitors who sent the letter to his wife had written to some further 600 people making the same

claim. The client had a wireless internet connection at home which he believed allowed misuse of their connection.

A Norfolk CAB client sought advice about whether a demand for £295 for the illegal download of a song was genuine. The copyright owners were claiming the client's internet connection had been used for the download.

Response to specific issues raised in the consultation

General questions

1. What should the priorities be for e-consumer protection?

We agree with the general approach and objectives suggested in the consultation. In addition, we are pleased to see the inclusion of several elements we have supported in the past, such as the need for pre-payment protection and for consumer protection agencies in the UK to embrace the full potential for working together, sharing intelligence and enforcement activity.

If problems with internet sales are to be tackled effectively, we believe that regulators and enforcers need to:

- join forces with consumers, so that intelligence on consumers' experiences is actively encouraged;
- create links between online feedback and advice and information from trusted sources such as OFT, BIS, Adviceguide and Consumer Direct;
- make full use of internet providers to block or take down the websites of traders that are fraudulent or persistently trading unfairly;
- reduce trader anonymity by requiring the seller to provide account details where payments can be made online by buyers;
- encourage internet service providers to check who the traders using their facilities are and provide this information when consumers enquire about trader identity, for example when a web site disappears. to vet their online practices;
- respond quickly to alerts from enforcers;
- strengthen pre-payment protection so that it is compulsory, as well as educating consumers about existing redress offered by some internet platforms; and
- provide consumers with key facts on rights, responsibilities, on-line security and which potentially detrimental practices to check and avoid.

2. Do you agree with the general approach of encouraging market based solutions supported by targeted enforcement, education, and influencing? Why or why not?

Yes, provided that markets are prepared to actively engage with stopping the problems that consumers' report. To provide real benefit for consumers, self-regulatory approaches need to recognise that:

- Consumers need extra layers of protection such as pre-payment and ID security to feel confident to make a purchase;

- Internet service providers have duties to consumers as well as to their business customers. Their name will be associated with any problems consumers experience and it is therefore in their own interests to provide facilities for consumers to tell them when things go wrong, so that they can ensure that bad practices are not repeated and that consumers can access redress; and
- Businesses who sell online have an extra layer of responsibility to ensure they comply with consumer protection rules in an internet environment. For example, to provide relevant, easily accessed and brief terms so that consumers know what they are agreeing to when they buy on line and can reference the terms later if something goes wrong.

3. Do you agree with the focus of the three areas of empowering consumers, promoting business compliance and making enforcement more effective? Why or why not?

Yes. The themes, proposed solutions and proposed actions follow the stated objectives for the planned e-consumer protection strategy and appear to be reasonably comprehensive.

For consumers to feel confidence in reporting their on-line problem purchases, we agree that there should be an online point of contact for consumers. This could then inform enforcement and consumer education. We also invite enforcers to access CAB evidence about online consumer problems.

In addition, we would expect to see the development of links and responsibilities between Trading Standards in the trader's home area and Trading Standards in areas where that trader sells online. Currently, a person who buys from a seller who lives in another authority may suffer if there is a problem and the seller is being uncooperative. Bureaux in Scotland report that this has been a particular issue for Scottish consumers in the islands north of the Scottish mainland, who are using the internet to access a wider group of traders than might be available locally.

4. Are there any key areas in relation to businesses or consumers that we are missing?

Yes.

Traceability and transparency are key to enforcement and to the access to redress that will boost consumer confidence. It is too easy for internet businesses to disappear and to ignore contact from consumers. Internet service providers should be required by enforcers to provide information on the identity of businesses when web sites disappear and contact details fail. Consumers could then use consumer gateway provisions under Part 9 of the Enterprise Act to access this information to enforce their rights.

It is also important that consumers are kept informed as to how their issue is being dealt with when a problem is reported to enforcers and the final outcomes.

Poor Traceability of online businesses can mean that consumers cannot easily discover whom they are dealing with online. For example, CAB clients have been contacted by businesses they do not know via what appear to be brokerage arrangements or different trading styles of the same business, as illustrated in the examples below.

When a CAB client from Leicestershire bought London theatre tickets online she ticked a box for a £10 voucher to spend in London. Later she discovered that a direct debit was being claimed from a voucher business who had already claimed £343.95 in payments. The company claimed she would have received a welcome email with their terms and conditions. The client had not seen any terms and thought it likely any such email would have been discarded as spam. She was adamant that she had not given her payment card details to the voucher company direct.

A CAB client in Staffordshire on income support sought a loan for Christmas presents. She paid nearly £50 to three different companies whose web sites said they could arrange a loan. The last one sent paperwork which she signed and returned only to find they then referred her to yet another firm who again sought nearly £50 but then claimed to have no knowledge of her application. All four used premium rate phone lines and she was unable to get her money back.

5. Are there any general comments you would like us to take into account when developing the e-consumer protection strategy?

Yes.

Consumer confidence has to be won and retained. In addition to educating consumers and raising expectations, businesses need to promptly address concerns that arise. Where a market is experiencing bad practice and enforcement is not prompt, it is too easy for others in that market to follow the bad practice. To avoid this, trade associations need to highlight the bad practice and actively encourage change, rather than waiting to see if a court decides there is an enforceable case.

Enforcement costs should be met by recalcitrant business. Where repeated inspection and enforcement is needed to ensure a trader trades fairly, that trader should be risk assessed and pay enforcers' costs of tackling that business's failure to comply with consumer protection law. This would reward businesses that respond to advice and take corrective action.

Restorative justice should be actively used in enforcement to compensate consumers when a business is found to trade unfairly.

Empowering Consumers

EC1. Besides providing advice and information, how else can we encourage consumers to report problems to the online reporting system? Would providing feedback on the outcome of their complaint be a strong incentive for consumers if it can be done cost effectively?

EC2. What other things should OFT do to fully utilise this online point of contact?

To encourage consumers to report problems, reporting facilities need to be available at the point where the complaint arises. Consumers are using online forums to tell other consumers about their experiences in relation to products bought online. Bureaux frequently report that they or their clients have found information about problems being experienced with a business by looking at online forum discussions. To harness this, information links could be provided to, for example, Consumer Direct.

We believe that where consumers report problems to regulators and enforcers, the reporting back of outcomes is crucially important. It values the information received, provides an opportunity for information and advice to explain the law and empower consumers to avoid the same outcomes in future. In addition, it informs consumers about the work of regulators and enforcers and what action can be taken.

Feedback need not be expensive for enforcers and regulators, it could be linked to outcomes on online complaints websites. That link should show whether the problem is under investigation. To allow enforcers to provide this feedback it will be important that Part 9 of the Enterprise Act, which prohibits them from sharing information gathered using their enforcement powers, is respected. We suggest that stipulating only the nature of the problem would avoid publicising the name of the business. When a case has been concluded, for example once an undertaking has been given or a court case concluded, press releases should include thanks to those whose evidence helped the case, such as consumers or other businesses.

EC3. What are the barriers to carrying out joint education/marketing campaigns?

EC4. Which organisations should be involved? Are businesses interested in becoming involved? How?

We agree with the objective for informing both consumers and business about consumer rights and responsibilities, if legislation is to work fairly. Whilst business may not initially agree that they need to educate consumers, we believe that this has been overtaken by existing legal requirements. For example, legislation for distance selling and the duty to trade fairly requires several pieces of information to be provided before the point of sale.

Key rights information which is simple, concise and prominent could both reassure business that they satisfy consumer protection requirements and inform consumers of their rights at the point where they need the information on the seller's website. We therefore do not see the rationale for barriers to joint education/ marketing.

Businesses who agree to joint marketing work should not, however, expect to receive favourable treatment from enforcement agencies if they fail in meeting consumer protection requirements.

EC5. Are there other tools that could assist consumers in seeking redress?

EC6. What barriers are there to consumers obtaining redress?

EC7. How could we ensure that Alternative Dispute Resolution processes are used by consumers, and taken seriously by business?

EC8. How can we encourage businesses to improve their complaints handling processes?

The barriers to obtaining redress are many and vary from consumer to consumer and between different purchasing methods. They include, for example, physical impairments, poor language skills and problems with access to transport to visit traders or return faulty goods. Complaint mechanisms are inadequate where the business fails to respond to complaints. Many cases reported by bureaux note that communications have not been answered. In other cases the trader cannot be found or has ceased to trade.

Ensuring ADR is used by consumers and business may require legislation, perhaps through an EU wide provision as indicated in the consultation at A34. Whilst provision of redress mechanisms has been recognised as essential in the utilities and financial sectors, there is no such requirement for all consumer goods and services. Citizens Advice has lobbied for a consumer ombudsman over the last ten years and suggested this again during consultations about the role of a Consumer Advocate. ADR often has advantages for consumers over taking court action in that: it is a less formal process; is quicker; and is usually funded through the business's licence to trade and a fee per case. The business has a financial and reputational incentive to resolve the case before it reaches the ADR stage.

It is unclear as to how businesses who do not provide adequate complaint handling processes online will be encouraged to do so unless it is a requirement, perhaps under the E-commerce Directive or as a provision of the Distance Selling Directive.

EC9. What do you or your organisation consider to be best practice to effectively target consumer education messages to those who need it?

In general terms, information and education material is most useful at the time it is needed. In the context of e-consumer protection, this would be prior to making a purchase and on making a complaint. Where education messages are provided, they also need to be easily found. Please also see our suggestions for templates of consumer information in the response to questions EC3 and EC4 above.

Best practice for effective targeting will vary in relation to the audience and the capacity of individuals to access the messages.

EC10. Do you agree that reviews or other research mechanisms are a useful tool for consumers? How can consumers be encouraged to use these prior to carrying out a transaction?

Yes. CAB evidence often states that consumers and advisers use information posted by others to confirm whether they have a case for complaint and whether the trader is still trading. To encourage consumers to check this feedback pre-purchase we suggest it forms part of the template of information suggested for web sites in response to questions EC3 and EC4.

EC11. How can we encourage consumers to share experiences in order to reduce collective consumer detriment online?

We believe that this frequently happens now via online forums. Sometimes where many consumers are experiencing the same problems, sites have been set up to warn and help other consumers, because regulators have failed to proactively obtain feedback from consumers.

EC12. How can we encourage businesses to make payment systems safer?

We believe that pre-payment protection needs to be compulsory and have suggested escrow, and a Scottish equivalent.

We suggest that the OFT could discuss with those companies detailed in paragraph A55 why they offer pre-payment protection and how their escrow works. This could inform a way forward and discussions with OECD, FSA, BIS and EC colleagues for improved protection.

It is vital that the pre-payments that are protected are not accessible to the business for their ongoing costs or indeed for meeting claims from secured creditors. The money needs to be deliverable to the consumers who paid it if it is to meet the objective to increase consumer confidence online.

EC13. How can we encourage consumers to transact more safely online?

Buying on the internet is associated with speed and important messages have to be simple, concise and prominent for consumers to take any notice. More written material seems unlikely to work since we know that people frequently fail to read terms and conditions. The existing symbols used for trusted sites are a good idea but do not seem to override the impulse to buy.

We believe that consumers need more help to achieve safer online transactions. Internet providers, payment card issuers, business and the regulatory and enforcement community also have a part to play in checking those who sell over the Internet.

EC14. What can be done to improve the information provided to consumers on instant cash transfers or the security arrangements relating to these payments?

This is a difficult problem that we have not, to date, been able to tackle successfully.

Promoting Business Compliance

Our responses in this section are given from a consumer perspective only.

BC1. Why do businesses not use guidance more often, and what can we do to encourage them to?

BC2. How can we make guidance on existing and future regulation in this area more accessible and user friendly (for example, are there exemplars we could follow and is there a specific location where guidance should be held such as Directgov, OFT website, etc)?

The research highlighted in the consultation suggests that the problems business face in their lack of knowledge about consumer protection law is similar to that for consumers. The first step is a perception that you need information and then the ability to access a trustworthy source that can be readily understood. For business, however, the law expects a degree of expertise that properly acknowledges the responsibilities of the role of the trader. All businesses need to have an acceptable level of knowledge about the laws that relate to that business, be they related to tax, health & safety, product specific requirements or consumer protection.

We agree that guidance to business on consumer protection needs to be consistent and suggest that the example of the OFT's Sale of Goods Act Hub should be repeated across other consumer protection legislation.

During discussions on the UK transposition of the Services Directive, Business Link was agreed as the portal for businesses to access the information they required. We suggest that Business Link, trade associations and the larger bodies such as CBI and BRC should also be provided with any links not already in use on their web sites.

The proposals for action in paragraphs B6 to B8, to build on past work and for all those with an interest to work together, seem sensible. We suggest that the OFT should also use relevant business journals, newsletters and conferences to disseminate information and to reinforce compliance requirement messages. These avenues need not be costly if the OFT supplies free materials and speakers.

BC3. Is the current level of consumer to consumer regulation sufficient, given the nature of the market?

BC4. If not, what additional essential consumer protection would be required?

The concept of providing for consumer to consumer legal protection obligations questions the accepted idea that business will have or has access to legal advice and that regulatory compliance is a business cost. We appreciate that sales from one consumer to another consumer do happen, for example in internet auction and classified advertisements web sites. We do not think that consumers should be barred from this activity, or indeed that it would be possible to do this, but do agree with the accepted practices for determining when the level of sales crosses into the area of trading as a business.

We suggest that the website advertisements for consumer to consumer sales should be marked as such, for example, by referring to information on the non-applicability of consumer protection rights or a straightforward warning to say that these offers are not from a business where consumer rights apply.

BC5. Other jurisdictions have positive reporting requirements (such as requiring businesses to provide information to authorities) – should the UK? What are the advantages and disadvantages?

BC6. Should the database generated by businesses about suspected fraud be searchable to contributing businesses? If not, what incentive is there for businesses to contribute?

We agree that intelligence sharing between regulators, enforcers and internet intermediaries should be facilitated. It would, we believe, help to tackle fraud quickly and inform consumer warnings. Action Fraud should be a key agency for this work.

BC7. Should the UK be using co-regulation more extensively to help shape consumer protection on the internet, or is self-regulation sufficient? Why?

Policing compliance is costly. All regulators, including local authority trading standards services, will be facing additional budget constraints. Co-regulation will, we believe, become more important in helping businesses who want to comply with the law to do so and in highlighting where enforcement is necessary. Further, the best practice guidance that is being developed through regulators and enforcers working with industry will be valuable in assessing the professional diligence required under the Consumer Protection from Unfair Trading Regulations (CPRs).

BC8. Given other challenges for UK internet enforcers, should the UK be doing more to reduce spam and if so, what?

BC9. Do you agree with the approach set out below (on spam)? Specifically who is best placed to do it, how and who should pay?

We agree that spam, and internet frauds and scams generally, are essential for better e-consumer protection. Again this would seem best tackled through a joined up approach by those with powers to take action on particular issues, including the National Fraud Authority. As indicated in the consultation, those enforcement authorities who can monitor where spam comes from and trace back to those responsible, those intermediaries who can remove the facility to send the spam, those who can access and confiscate the financial gains and those who can warn consumers also need to take an active role. We appreciate that sending and receiving spam will not be confined within one country. Consequently, international assistance will be needed. Even though this is a difficult task, we cannot afford not to tackle it.

BC10. Should the OFT be focusing effort on inspections and web sweeps (using software tools where appropriate)? What other approaches could we take and why?

The consultation suggests inexpensive standard response letters for non-compliance and expensive web crawlers. We agree that where OFT and Trading Standards have undertaken web sweeps to check compliance, the results will alert some businesses to tackle compliance failures they were not aware of. We are, however, concerned whether standard letters will be followed up. If they are not, the message that failure to comply with the law will have consequences is lost.

Fraudsters are generally quick to use all opportunities as and when they arise so that using the latest technology, such as web crawlers seems to be a necessity.

Enforcement

Citizens Advice and Citizens Advice Scotland are not enforcement bodies. We have therefore responded to this section in general terms but have answered question E19 specifically.

General comments

We agree that the enforcement focus needs to include:

- internet enforcement capability;
- cross-border enforcement;
- monitoring for developments and for whether legislation remains effective;
- minimising duplication through co-ordinated action;
- establishing and maintaining a UK e-consumer protection enforcement group; and
- increased data sharing and intelligence gathering.

We note from the consultation document that several initiatives are already being used to tackle internet enforcement across consumer protection legislation and fraud and other illegal practices. It is clear that there is a range of important UK and international partners and we see that it is essential that close links are maintained. A regime where cross

border enforcement and support from enforcement agencies with differing remits would seem essential.

Clearly joint working will require sharing of intelligence to avoid duplication and maximise outcomes. Legal challenges about information sharing will need to be examined and resolved so that they do not create unnecessary bars to tackling the problems and thus play into the hands of those engaged in criminal activities.

Training and clear jointly held approaches for assessing detriment and deciding on appropriate levels of enforcement will, we agree, be essential too. We agree with the proposals being developed in diagram C1. The suggestions for interworking and shadowing also seem sensible.

In addition to data from Consumer Direct, cases reported by bureau advisers across England and Wales can be searched for further information on the issues and problems that consumers are experiencing. We are happy to help enforcers in their work where this database of cases is of value. In Scotland we are happy to continue to work with the OFT on consumer issues that effect clients.

E19. Is the OFT the right body to coordinate and analyse consumer protection intelligence arising from the various sources that exist?

We think that the OFT should have this role as part of their role as the UK lead and conduit for the Consumer Protection Co-operation Regulations for EU cross border enforcement and in their role with ICPEN. However, clear protocols will need to be in place with other enforcers, such as the National Fraud Authority, to tackle internet fraud.

Monitoring the strategy and developments in online markets

M1. Do you agree with our approach to monitoring the impact of the strategy and wider developments in online markets?

M2. Do you agree with the anticipated outcomes we expect to achieve from the implementation of the proposed actions?

Yes. The tables in this section appear to reflect the objectives for the strategy. We have one suggestion, that evidence from consumer bodies should be used as an indicator of whether education, empowerment and enforcement work has been successful and to assess the need for further input.

If you have any queries in relation to this response please contact Susan Marks on 0207 833 7132 or at susan.marks@citizensadvice.org.uk

Citizens Advice is an operating name of The National Association of Citizens Advice Bureaux. Registered charity number 27905

The Scottish Association of Citizens Advice Bureaux - Citizens Advice Scotland
(Scottish charity number SC016637) Copyright © Citizens Advice Scotland, 2010

www.citizensadvice.org.uk

www.cas.org.uk