

Financial Services Authority

The FSA's approach to the regulation of e-commerce

June 2001



Contents

1	Executive summary	3
2	Introduction	10
3	Principles underlying the FSA's approach	13
4	International context	19
5	Review of e-commerce risks	25
6	Approach to Information Technology (IT) risk management	31
7	Approach to consumer security	44
8	Approach to information for consumers	51
9	Adapting the regulatory approach	69
	Annex A: FSA's existing work and initiatives	
	Annex B: International fora	
	Annex C: Internal developments in the FSA	
	Annex D: On-line finance consumer messages	
	Annex E: Consideration of .fin as a tool of supervision	
	Annex F: Questions	

The FSA would welcome comments on this discussion paper. Comments should reach us by 30th September 2001.

Please send comments by electronic submission using the e-mail address :
e-commercetheme@fsa.gov.uk

Alternatively, comments may be sent in writing to:

Internet Unit
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

It is the FSA's policy to make all responses to formal consultation available for public inspection unless the respondent requests otherwise.

1 Executive summary

What underlies the FSA's approach to e-commerce?

- 1.1 E-commerce¹ opens up substantial new opportunities for consumers and the financial services industry. The FSA welcomes the competition, the potential for cost-savings and the increased choice this may bring to consumers. Consumers can benefit from the increased amount of information available and the ease with which this may be accessed. Firms and consumers may benefit from the lower cost base and greater speed to market. Firms can also use e-commerce to extend their customer base. In addition, increased automation provides the opportunity for fewer individual human errors. E-commerce also creates the potential for better audit trails and automated controls.
- 1.2 The FSA is looking to exploit the opportunities available to it in the areas of consumer education and the possible use of new technologies to improve the economy and efficiency of regulation, for example using the Internet and web-based software to enable on-line interaction with firms. This discussion paper, however, focuses primarily on the challenges posed by the use of e-commerce channels to the achievement of the FSA's statutory objectives. These objectives,² which underpin the FSA's work, are:
 - a) maintaining market confidence;
 - b) promoting understanding of the financial system;
 - c) protecting consumers; and
 - d) reducing financial crime.

One of the key challenges for the FSA is how to address the risks posed by e-commerce in a way that allows the potential benefits, including competition and innovation, to flourish.

1 E-commerce will be used to refer to financial service provision using the Internet and other web-enabled technologies, including wireless application protocol, other mobile telephony systems, and interactive digital television.

2 The objectives are contained in sections 3-6 of the Financial Services and Markets Act 2000 (FiSMA).

- 1.3 The FSA does not have a monopoly of interest in these objectives, nor can they be solely achieved by its efforts. Nonetheless, the FSA has a critical role to play because by establishing expectations, norms and responsibilities it can help create an environment in which appropriate standards are maintained. For this reason the FSA is actively seeking a dialogue with its stakeholders, including senior management of financial firms, trade associations, consumer bodies and government on the broad issues raised in this paper. The FSA is also looking for responses to the specific questions asked throughout the document. Some of these issues are of a more technical nature and may be of interest to a more specialist audience.
- 1.4 Beside the statutory objectives, the FSA's approach to e-commerce takes into account the principles of good regulation. Particularly relevant to e-commerce are:
- a) the role of senior management in meeting the challenges of e-commerce;
 - b) facilitation of innovation by avoiding unnecessary barriers to launching new financial products and services;
 - c) the need to have regard to the international character of financial services and markets and the desirability of maintaining the competitive position of the UK;
 - d) the minimisation of any adverse effects of regulatory decisions on competition; and
 - e) a proportionate regulatory approach.
- 1.5 The FSA has also adopted a policy of technological, or delivery channel, neutrality. This policy means that the FSA will not discriminate in its approach on the basis of delivery channel alone, unless the risks to the statutory objectives from different delivery channels justify it. Technological neutrality does not mean that the same specific requirements must be imposed on all delivery channels, since the risks related to doing business via the telephone, Internet, or post may be different. This policy has been formulated to address the concern that the use of new technologies might result in disproportionate regulation being imposed in some areas, while in other areas important risks might be overlooked.³ Technological neutrality is discussed in greater detail in chapter 3.

3 The potential interim impact of the European Union's Electronic Commerce Directive (ECD) is discussed in Annex B.

International context

- 1.6 One of the key features of e-commerce is that it is a global communications and delivery channel. It is technically possible for firms based anywhere to provide services everywhere. Globalisation challenges the traditional way in which countries exercise control over the provision of financial services and makes international co-operation crucial. It is for this reason that the FSA (along with other regulators) is playing an active role in those international fora that are considering e-commerce. Without taking an active part in shaping the international structure of regulation, the FSA would be impaired in its ability to meet its domestic statutory objectives. Chapter 4 and Annex B of this paper provide details of some important issues that are being discussed in the international fora in which the FSA takes part.

Focus of the discussion paper

- 1.7 A considerable amount of work has been done by the FSA and its predecessor organisations over the last few years to respond positively to the use of the Internet and other web-enabled technologies. This work is described in Annex A. Last year the FSA announced a review of its approach to the regulation of e-commerce as one of its four themes. This project has sought to identify and then prioritise risks related to the use of e-commerce channels that might prevent the FSA achieving its statutory objectives. Many of these risks are not unique to e-commerce. Nonetheless, even where the risks do not arise only from the use of e-commerce delivery channels, their use may increase or reduce the significance of these risks. An assessment has been made of areas where additional work is needed to bridge the gap between the identified risks and existing work to manage them. The assessment is summarised in chapter 4.

Conclusions of the review

- 1.8 The assessment that has been carried out indicates that further action is needed by the FSA. This work may be grouped into three areas. These are that:
- a) firms and markets have adequate IT systems and controls to address the risks in their business (see chapter 6);
 - b) consumers have access to relevant and comprehensible information and guidance about obtaining financial services via e-commerce channels; and consumers appreciate that, once armed with this information, they have a responsibility to protect themselves from the risks they can best manage (see chapter 7 and 8); and

c) the FSA adapts regulation to e-commerce developments (see chapter 9).

- 1.9 Although this paper identifies actions which the industry, consumers and the FSA should consider, one of the common themes that runs through the analysis is that no one group can do everything. Achieving appropriate standards in this area, as in many others, is a shared responsibility in which roles interlock. As the discussion of consumer security makes clear, neither firms nor consumers can completely counteract a failure to maintain proper controls by the other (see chapter 7).
- 1.10 Paragraphs 1.11 – 1.19 below contain a summary of the proposals in each of the three key areas in paragraph 1.8.

Adequate IT systems and controls

- 1.11 For the majority of firms and markets, IT provides the backbone of the business, whether or not the firm uses e-commerce delivery channels. It is not the FSA's job to specify in detail what systems and controls a firm should use. That is the responsibility of its senior management. However, the FSA can make clear its expectation that senior management is responsible in this area and that the controls which are in place should adequately address the risks to which the business is exposed. Chapter 4 sets out how the FSA might clarify its expectations and promote adequate standards in this area.

Consumer security and information

- 1.12 E-commerce is likely to provide consumers with more opportunities than risks, but consumer security and appropriate information are key.
- 1.13 Consumer security has always been important; for example consumers have to keep secret the PIN number on their credit, debit and cash cards. In the past firms themselves were able to control security in the delivery channel; they could secure their own machines, the communications link to ATMs or other remote devices and the remote device itself. The use of e-commerce channels reduces firms' end-to-end control of security.⁴ It is the consumer who controls access to his computer and it is the consumer who can take steps to secure it. The FSA believes that consumer security is a shared endeavour between firms, consumers and the FSA. The FSA plans to publicise what consumers can do to reduce the risk that they compromise their own security when using e-commerce channels. This is discussed in chapter 7 and Annex D.
- 1.14 Good quality information is a key requirement if consumers are to select material sensibly from the abundance of data in cyberspace. Information needs to be presented in a way that consumers can understand. The specific

⁴ For example, banks own and control the ATM network, this is very different from the position of on-line banking. However, for other services such as stockbroking, the use of e-commerce delivery channels may provide greater levels of security in some circumstances than the use of traditional communication, such as post or telephone.

qualities of different delivery channels need to be understood when the FSA is revising disclosure requirements. The FSA is one of a number of organisations with responsibilities to provide general consumer financial information. As a regulator, the FSA can play a valuable role in helping consumers become aware of what protections exist within the UK, of the circumstances in which consumers may not be covered by UK regulatory protection, and the potential consequences of not being so covered. The FSA can also provide independent information to help consumers make an informed choice about obtaining financial services. Chapter 8 sets out the specific areas in which the FSA could provide such information.

Adapting the UK regulatory framework

- 1.15 The growth of e-commerce has seen the development of new products with new risks and also of novel solutions to mitigate risks. Two new services have received particular attention: aggregation and digital certificates supporting electronic signatures.
- 1.16 Aggregation is a new service. It enables a consumer to be presented with all his or her account details (banks, stockbrokers, air miles etc) on a single page. The most common method of aggregation currently requires consumers to provide their account passwords to the aggregator. The aggregator uses the passwords to access automatically the consumer's accounts. The information is then provided to the consumer on a consolidated basis on a single page. This paper clarifies the FSA's approach to aggregation in a number of important areas. These are:
- a) that accessing data from a variety of sources and consolidating the information onto a single web page is not regulated under financial services legislation, although services an aggregator may choose to add to its site, for example providing investment advice, or arranging deals, may trigger an authorisation requirement;
 - b) as with any new business activity, authorised firms planning to undertake account aggregation are expected to undertake appropriate levels of due diligence, in particular on the legal issues relating to certain methods of aggregation where the law has not been tested.⁵ Authorised firms should seek legal advice from an expert and reputable source and should not provide aggregation services if the advice received is that any aspect of their business model is more likely than not to be illegal, even if prosecution is believed to be unlikely; and
 - c) a consumer who decides to use an aggregation service which asks the consumer to disclose his or her password, should check very carefully that

⁵ Relevant legislation includes the Computer Misuse Act 1990, the Copyright Designs and Patents Act 1988, the Copyright and Rights in Databases Regulations 1997 and the Data Protection Act 1998. Aggregation does not fall within the scope of Financial Services and Markets Act 2000 (FiSMA).

he or she is not breaching an account provider's terms and conditions, and whether the level of security provided by his or her on-line bank or investment firm will be diminished by that use.

These issues are discussed further in chapter 9. The FSA is conscious that, as with any new and dynamic service, legal certainty may not always be possible.

1.17 Digital certificates supporting electronic signatures are widely believed to be an important building block in the development of e-commerce. European law prevents Member States from requiring firms providing digital certificates and other trust services to be authorised. However, voluntary accreditation and other schemes are encouraged and are being set up. Under the law, therefore, any firm (financial or non-financial) is free to warrant that a particular person is who he or she purports to be for the purposes of a specific transaction. The key issue for a firm relying on such a warranty is the need to appreciate that not all those who provide certificates are equally reliable. Firms will need to develop procedures for determining how much reliance may be placed on a particular certificate. The discussion paper poses a number of questions about:

- a) the standards that would have to apply in this area before certificates could be used for the purpose of entering into a financial relationship;⁶
- b) the issuing of digital certificates by authorised firms;
- c) the acceptance by authorised firms of digital certificates issued by others;
- d) the use by authorised firms of digital certificates in the course of business; and
- e) the use of electronic signatures by consumers.

These issues are discussed in paragraphs 9.16 – 9.55.

1.18 An example of where the Internet can provide a novel solution to risk is in the possible use of domain names. A financial domain name could be used to help consumers identify whether or not a firm is authorised. Consumers can and should check with the FSA's Central Register, but currently not everyone does. A special Internet address (for example .fin) reserved for financial services firms, and possibly made compulsory for them to use, might be one way of mitigating that risk. This could also help regulators conduct surveillance more effectively, since an unauthorised .fin web-site would be relatively easy to uncover.

1.19 There are two versions of the .fin approach. One is for a sub-level domain, i.e. www.firm.fin.uk, the other is for a top-level domain, i.e. www.firm.uk.fin. The paper analyses the advantages and disadvantages of the use of .fin as a

⁶ This work was done in conjunction with the Money Laundering Theme. See separate discussion paper about money laundering published in June 2001.

top-level domain because ICANN, the agency that controls such domains, has indicated that it is willing to authorise its use. This review has concluded that the difficulties and costs associated with operating a financial top-level domain are not currently justified by the prospective benefits. However, the balance between costs and benefits can be expected to change over time. This is an issue to which the FSA may wish to return. The analysis is covered in paragraphs 9.56 – 9.64 and Annex E.

Other challenges and opportunities

- 1.20 This paper also reviews the challenges and opportunities the Internet and other web-enabled technologies present for the way the FSA goes about its business as a regulator. These are discussed in Annex C.

Way forward

- 1.21 The FSA seeks feedback on the issues raised in this paper to help it develop an appropriately balanced regulatory response. A list of the detailed questions in the paper is contained in Annex F. Responses should be made by end of September 2001 either by email to e-commercetheme@fsa.gov.uk, or by post to the Internet Unit, 25 The North Colonnade, Canary Wharf, London, E14 5HS. A conference on e-commerce will be held by the FSA in June 2001 where initial reactions and questions may be raised.
- 1.22 This paper is the beginning of an ongoing dialogue the FSA wishes to have on e-commerce matters. This year the FSA has set up an E-Business Advisory Group, containing both industry and consumer body representatives. This forum will provide a mechanism for continuing discussion between the FSA, firms and consumer bodies on e-commerce issues affecting regulation.

2 Introduction

- 2.1 This discussion paper looks at the provision of financial services via the Internet and other web-enabled technologies, such as mobile telephony and interactive digital television.¹ It does not discuss electronic money, nor the delivery of financial services by other electronic means, such as automated telephony systems.
- 2.2 The discussion paper considers e-commerce in light of the FSA's four overarching statutory objectives contained in sections 3-6 of the Financial Services and Markets Act 2000 (FiSMA). These statutory objectives are to:
- a) maintain confidence in the UK financial system;
 - b) promote public understanding of the financial system;
 - c) secure an appropriate degree of protection for consumers; and
 - d) reduce financial crime.
- 2.3 The rapid growth in the use of the Internet² presents many opportunities in the realm of financial services for providers, consumers and regulators alike. For providers, there is the opportunity to reduce costs and offer services to a potentially wider range of customers than would previously have been cost effective. For consumers, there is the potential to compare products more quickly and economically. For regulators, there are opportunities to reach a wider range of stakeholders through the use of web-sites and to protect the public by conducting surveillance of the Internet.

1 In the interests of brevity, the word Internet will be used in this document, to refer to the 'Internet and other web-enabled technologies, including wireless application protocol, other mobile telephony systems, and interactive digital television', unless the sense indicates otherwise. Similarly, e-commerce will be used to refer to financial service provision using all these technologies.

2 The National Statistics Omnibus survey (March 2001) stated that 51 per cent (i.e. 23m) of UK adults accessed the Internet at some time during January 2001, 23 per cent of these used the Internet for personal banking, financial and/or investment activities. The Omnibus survey also notes that over the fourth quarter of 2000 an average of 8.6m households (35 per cent of all households) in the UK could access the Internet from home. This represents an almost four fold increase in two years.

- 2.4 The focus of this paper, however, is not on the important opportunities which the Internet provides. Instead, it seeks to identify those e-commerce related risks which might prevent the FSA achieving its four statutory objectives, and to discuss ways in which these risks could be mitigated. The paper reflects a new FSA approach, one designed to supplement the individual supervision of firms with more frequent thematic and peer group reviews.
- 2.5 The Internet not only creates opportunities that did not exist cost effectively before, it also increases the significance of a number of risks which were not previously material, or at least not to the same extent. In summary, these risks and opportunities arise because:
- a) the Internet is a global medium, raising difficult practical issues concerning jurisdiction;
 - b) the Internet is a virtual medium, which permits a service to be provided at a significantly lower cost and with a less extensive physical presence, with clear implications for money laundering controls, for the non-face-to-face provision of services, such as the provision of investment advice, as well as for the cost structure and level of competition within an industry; and
 - c) the Internet harnesses the power of computers, and brings with it four important consequences:
 - (i) an increase in the speed of transactions, and in the amount of information available to firms, markets and consumers;
 - (ii) the need for greater discrimination on the part of consumers faced with large quantities of information and the possibility of different patterns of consumer purchasing behaviour depending on the particular medium;
 - (iii) an expansion in the number of market participants as smaller firms and private individuals gain access to information and trading strategies which previously only the largest firms have enjoyed; and
 - (iv) a greater reliance on technology and its associated vulnerabilities.
- 2.6 A further consequence of bringing together the power of computing and of global telecommunications is that the Internet is re-engineering business processes and restructuring industries. It is enabling new players (including non-financial firms) to enter the financial market. It is reducing costs, increasing choice, permitting disintermediation, and shifting the balance of power within the group of providers that collectively deliver a service, as well as between providers and receivers of a service.
- 2.7 The FSA is not concerned with all risks – nor is this paper – only with those which would prevent it from meeting its statutory objectives. Thus the mere fact that increased competition might lead some firms to fail or be taken over

is a risk for particular firms, but would not necessarily compromise the FSA's achievement of its objectives. It would not do so because:

- a) regulation is not designed to prevent market forces from operating;
- b) in exercising its powers the FSA is required to have regard to the desirability of competition;
- c) commercial failure could be evidence that competitive markets are operating; and
- d) the FSA does not operate a no failure regime.

2.8 On the other hand, should radical restructuring, or widespread firm failures, or large scale Internet security problems be such as to lead to loss of market confidence or consumer detriment, then these would become risks which the FSA would need to address.

2.9 Much of the work which the FSA has done in this thematic review over the last year has been concerned to differentiate, and then prioritise, those e-commerce related risks which might prevent the FSA achieving its statutory objectives, from those risks which are the responsibility of firms, consumers or markets to manage. Extensive mapping and analysis of such risks has led to the identification of 17 risks as being of the highest priority. This review and a summary of the 17 priority risks identified are contained in chapter 5.

3 Principles underlying the FSA's approach

- 3.1 The FSA's approach to e-commerce is necessarily governed by the Financial Services and Markets Act 2000 (FiSMA), which gives the FSA four statutory objectives.¹ The first, maintaining confidence in the UK financial system, is relevant to e-commerce because the dissemination of rumour and fact through Internet news bureaux, bulletin boards and chat rooms may well reduce the time available for firms and regulators to deal with a systemically significant event and also reduce the quality of information on which decisions need to be based. In addition, a major e-crime or security incident could lead to a loss of confidence in the Internet as a medium and subsequently to a major disruption of a financial market or sector.
- 3.2 The FSA might fail to meet the second objective, promoting public understanding of the financial system, because the Internet and web-enabled technologies are likely to change the landscape of the financial services industry and challenge consumer understanding of the financial system.
- 3.3 The third objective, securing an appropriate degree of protection for consumers, might be threatened by the global and virtual delivery of financial services, which creates a new environment in which IT security risks and the risks of doing business with firms operating from other countries have the potential to lead to consumer detriment.
- 3.4 The FSA in pursuing the fourth objective, reducing financial crime, has to address the opportunities which e-commerce presents to criminals. These include: attempts to manipulate regulated markets through the use of bulletin boards and chat rooms, attempts to launder money using Internet banks or e-money, promoting scams and frauds over cyberspace, and stealing money from on-line accounts.
- 3.5 In exercising its regulatory functions, the FiSMA also requires the FSA to have regard to a number of factors, known as 'the principles of good regulation'.

¹ The FSA can only be directly interested in those aspects of e-commerce that are regulated activities. Some aspects of e-financial services will fall outside its direct scope, for example, account aggregation.

Some of these are highly relevant to e-commerce. They include: the desirability of facilitating innovation, maintaining the competitive position of the UK, minimising the adverse effects on competition arising from FSA acts, facilitating competition between regulated firms, and proportionate regulation.

- 3.6 The FiSMA and the risk based approach to regulation set out in the FSA's strategic review, '*New Regulator for a New Millennium*',² have provided the general framework for the thematic examination of e-commerce undertaken over the last year. But the FSA's approach has also been informed by the policy of technological, or delivery channel, neutrality.
- 3.7 This policy has been adopted for three reasons, each of them identified by the International Organisation of Securities Commissions (IOSCO) as a guiding principle for e-commerce regulation. These are:
- a) *The fundamental principles of regulation remain the same whatever the medium.* In the UK that would include the reason why regulation is applied to certain financial services, the requirement for the FSA to meet its statutory objectives, the matters to which the FSA must have regard in exercising its general functions, the methods or tools which the FSA deploys, and a number of process disciplines, for example the requirement to consult before making rules or issuing guidance and the specific obligation (section 155 of the FiSMA) to estimate the costs and analyse the benefits of any proposed rule change.
 - b) *Consistent with these principles, regulators should not unnecessarily impede the legitimate use of the Internet by market participants and markets.* It is, after all, not in the public interest for countries and their regulators to distort the operation of the free market by imposing requirements that prevent firms and their customers doing business in ways that suit them, for example by taking advantage of new technologies.
 - c) *Regulators should strive for transparency and consistency regarding how their regulations apply in an Internet environment.*
- 3.8 Technological neutrality is not a legal requirement. It is a policy preference which informs some of the FSA's process disciplines. Thus if a situation were to arise in which the pursuit of this policy were in conflict with the achievement of the FSA's statutory objectives, the principle could be disapplied generally or on a case by case basis.

2 This review can be found on the FSA's web-site <http://www.fsa.gov.uk/pubs/policy/p29.pdf>.

Defining technological neutrality

- 3.9 A policy of technological neutrality bears a number of meanings. It may be understood in terms of requirements, in terms of processes, of outcomes or of principle. It is therefore important for the FSA to make clear what this policy does and does not mean. The policy means that the FSA will not discriminate in its approach on the basis of delivery channel alone, unless the risks to the statutory objectives from different delivery channels justify it.
- 3.10 The policy of technological neutrality does not mean:
- a) applying the same requirements to the same activity regardless of the channel employed;
 - b) replicating the same requirements for every channel, regardless of whether that medium presents the same risks; or
 - c) applying the same outcome measure, regardless of medium.³
- 3.11 Conversely the FSA would be complying with this policy if it:
- a) recommended standards of best practice for operators of on-line investment bulletin boards and chat fora;
 - b) conducted a review of Internet security by firms, but not of the purely physical security of a firm's off-line services;
 - c) imposed higher or lower capital requirements for on-line providers based upon experience of operational, credit or market risk profiles; or
 - d) developed anti-money laundering requirements that met the characteristics of e-commerce.
- 3.12 The policy of technological neutrality does not prevent the FSA from discriminating in its approach – for example in rule making, intensity of supervision or in consumer focused work – solely on the basis of delivery channel, if the risks to the FSA's statutory objectives justify it. This has four implications for the FSA's approach:
- a) non-discrimination does not suggest the imposition of the same requirements on all delivery channels, since the risk and/or control environments of delivery channels may differ and may therefore require recourse to different regulatory approaches. Nor does it prevent the FSA from taking medium-specific action to address a risk arising from the use of a particular communications channel. But it does require the FSA to be able to justify any differences by reference to the features of that specific medium;

3 Where monitoring compliance is not easy via one delivery channel, for example in the provision of face-to-face investment advice, the policy of technological neutrality would not prevent the FSA from developing an effective approach for another medium, so long as such an approach was designed to meet a statutory objective, core requirements or core standards of protection and was feasible and justifiable on cost benefit grounds.

- b) in pursuing the approach of technological neutrality the FSA will have to consider, for example the effect that a general requirement may have on different delivery channels. It is not enough to impose a general requirement that applies to all media, since this may be discriminatory. Delivery channel specific cost-benefit analysis will, therefore, need to be considered wherever it appears that the compliance cost of meeting a general requirement in one delivery channel may be significantly greater than in others;
- c) the FSA will need to provide for the same overall risk-based intensity of supervision, investigation, enforcement and consumer focused work, regardless of delivery channel. So, for example, it would not be technologically neutral to devote greater levels of regulatory attention to a particular channel, solely because it was easier to monitor activities in cyberspace. To do so would adversely affect competition. Whereas, paying greater attention to a medium because the risks were greater would be in line with a technologically neutral approach; and
- d) operating a policy of technological neutrality involves the FSA in identifying the particular risks associated with a specific technology, assessing the impact and probability of a risk crystallising, seeing how cost effectively such risks are currently addressed by the FSA, and taking whatever action might be needed to ensure that appropriate standards are maintained.

Legal and regulatory application

- 3.13 Technological neutrality is not a new aim for the FSA or its predecessor organisations. Technological neutrality is achieved at the statutory level, in that an activity which triggers a requirement for authorisation will do so whether the activity is performed face to face, by post, telephone, or in cyberspace. In this sense the law is technologically neutral.⁴
- 3.14 Another example may be found in the conduct of business arena, where regulators have made clear that pursuing a policy of technological neutrality has required rules to be waived or modified which have the effect of preventing firms and their clients from using technology in ways they wish to and where there are no consumer protection reasons requiring existing requirements to be rigidly enforced. For example, the requirement on stockbrokers to send contract notes to their off-line clients by mail is modified in the on-line world by permitting firms to give their on-line clients access to a secure part of the firm's web-site where they can collect their contract notes.

⁴ The extent to which the single market provisions of the EU's Electronic Commerce Directive will lead, in the short term, to a derogation from the principle of technological neutrality at the legislative level is discussed below at paragraph 3.16 and in Annex B.

The high level requirement is for clients to obtain confirmation of trades, and this requirement is met in different ways depending on the delivery channel employed. In the prudential arena technological neutrality has been embodied in core requirements such as that firms must have adequate systems and controls for all aspects of their business, given the nature and scale of their risk.

Issues arising

- 3.15 **Innovation.** A policy of technological neutrality could be interpreted as being in conflict with a number of principles of good regulation, such as the desirability of facilitating innovation, to which the FSA must have regard (see paragraph 3.5). For example, maintaining the competitive position of the UK might demand a proactively supportive regulatory environment for e-commerce – on the face of it, not an illustration of technological neutrality in operation. Similarly, facilitating innovation could easily be seen as being in conflict with technological neutrality, since to desire innovation is not to be neutral about it. However, while having regard to the desirability of innovation and competition, the FSA must nonetheless still meet its statutory objectives. One can be in favour of innovation without discriminating in favour of it.
- 3.16 **Europe.** The European Union’s Electronic Commerce Directive (ECD)⁵ represents a significant interim exception to the ideal of technological neutrality.⁶ A consequence of this Directive is that the requirements which a service provider from another EU Member State has to meet in a non-face-to-face interaction with a UK client may depend on the technology used: if the telephone or post is used, the marketing and disclosure requirements will be those of the country where the recipient of the service is based.⁷ If the same service is made available via a web-site or by e-mail, the service will be governed by the ECD, and the requirements will, with certain exceptions, be those of the country where the provider of the service is based. Where a firm uses both on and off-line channels the Directive will apply to the on-line channels and not to the off-line ones. A UK consumer obtaining financial services from a firm operating from another Member State will find that many of the marketing requirements with which the firm must comply, and hence the strict comparability of information on the site with that of UK providers, will depend on the technology used in the provision of the service. It is worth noting that the Commission is aware of the anomalous situation created by

5 European Directive 2000/31/EC.

6 A description of some of the ECD’s provisions is contained in Annex B.

7 Where the service provided is investment advice, an European Economic Area firm would have to comply with UK requirements relating to the provision of advice. See the discussion in chapter 4 and Annex B.

the Directive and in its recent Communication on '*E-Commerce and Financial Services*' (February 2001) proposes extending the country of origin approach adopted for e-commerce to other non-face-to-face channels.

Conclusion

- 3.17 This chapter describes the statutory requirements and within this framework the policy preferences of the FSA. It has discussed what technological neutrality means to the FSA (and its predecessor bodies) and how regulators have, in practice, implemented a policy of technological neutrality.
- 3.18 As discussed, the policy of technological neutrality does not mean that the FSA will never discriminate in its approach to a firm or an issue solely on the basis of delivery channel. Indeed, there will be times when to not discriminate between delivery channels would be detrimental to the achievement of the FSA's objectives, and thus its stakeholders, not least because different delivery channels will have different risk profiles. It does mean that where the FSA does discriminate there are clear reasons for doing so.

4 International context

- 4.1 Regulation may be designed to control the firm, the product or the selling process. In any cross-border provision of financial services, it is conceivable both for the country where the firm is based and for the country where the recipient of the service is based to assert regulatory jurisdiction. So where services are provided cross-border, both countries face the question as to whether they will both seek to authorise and then regulate the firm, product or activity or whether they will divide responsibilities between them in some way. Because the Internet is a global medium, which necessarily has to interface with national jurisdictions, or in some cases, such as the EU, transnational or multinational ones, the question of regulatory jurisdiction is a real and important one.
- 4.2 However, the question of which country is responsible for the regulation of which aspect of an activity is far from being the only jurisdictional issue that may arise. If there is a dispute, which country's courts have jurisdiction to try a case and which country's law they apply, are likely to be highly important to the litigants. There is also the question of the extraterritorial application and enforceability of the criminal law, for example on insider dealing or the making of misleading investment statements, and of any civil law provisions against market abuse, breach of which may result in the UK, for example in unlimited fines.
- 4.3 The rules of public and private international law were developed before the Internet age. It would be surprising if they were attuned to the ideal of a virtual global village. From that perspective there would be considerable attractions if the international community were to decide to develop a single set of requirements that applied across the world and which replaced national rules: consumers could shop on-line in confidence that the same standards and protections applied everywhere, while firms would not need to spend considerable sums of money adapting their web-sites to meet the requirements of every jurisdiction in which they operated.

- 4.4 Within the European Union significant progress is being made towards harmonisation through the development of the single market, based on a common set of core regulatory requirements within a binding legal environment. The Electronic Commerce Directive (ECD) will further enhance the single market by permitting a firm to provide services across the European Economic Area (the EEA) subject, broadly speaking, solely to the requirements of the Member State from where that service is provided, the so called ‘country of origin’ approach. One consequence of this approach is that it restricts the Member State where the recipient of a service is based from imposing its own requirements on providers based elsewhere in the EEA. However, the ECD applies only where services are provided via the Internet and e-mail, and then only to the pre-contractual phase. There are a number of other situations in which the Directive’s single market provisions do not apply. The Commission has recently proposed a broad strategy that would remove these derogations,¹ extend the ‘country of origin’ approach to all non-face-to-face media, enhance EU-wide redress mechanisms, and possibly in time provide for the harmonisation of financial service contracts.
- 4.5 In much of the rest of world, however, the ideal of global harmonisation of regulation confronts political, historical, cultural and legal realities. Politically, protecting consumers and maintaining confidence in markets are widely seen as central functions of the nation state. Historically, the kinds of protection and the standards of protection afforded to consumers differ from country to country because these standards have developed in response to specific problems. Culturally, the type of products and the different ways in which they are sold vary and may therefore create the need for specific regulatory responses; and, legally, different tests are used by countries to determine whether or not a service provided elsewhere is subject to their requirements.
- 4.6 The following are examples of some important differences between countries in the area of regulation and thereby provide the background for explaining the FSA’s strategic approach in this area.
- a) Different countries do not subject the same activities to regulation. For example, firms providing investment advice or dealing in commodity derivatives must be authorised in the UK, but do not need to be in some other countries. Conversely, providing credit triggers an authorisation requirement for a banking license in some countries, but not in the UK.²
 - b) Detailed regulatory requirements and protections frequently vary from one country to another, even when the same activity is subject to regulatory oversight. For example, the requirements relating to financial promotions, such as disclosing the level of charges and the effect of these on the performance of a packaged product, like a unit trust, vary from

1 i.e. exemptions from the requirements.

2 Provision of consumer credit is subject to the Consumer Credit Act which is operated by the Office of Fair Trading.

country to country and this makes product comparisons and informed choice difficult. Levels of compensation that are paid in the event of a financial services firm failing also vary widely, as does the coverage of any such compensation scheme.

- c) There is considerable variation in the tests applied by countries in determining which requirements must be complied with by an overseas firm marketing its services to people in another country. The UK and a number of leading countries operate a differential regime in which controls are disapplied where an overseas person is marketing or providing services to professional counterparties, i.e. those who either have, or can acquire, the expertise to conduct their own risk assessment.
- d) Where foreign firms have overseas consumers as their clients, countries adopt a variety of approaches. Some impose an authorisation requirement, unless the consumer solicits the transaction or service. Other countries impose only their marketing controls, such as disclosure requirements. An authorisation requirement would not be triggered unless the service is viewed as taking place within the country where the customer is based. In the UK, for example, custodial services and managing funds typically take place in the country where the provider of the service is based, while providing loans or investment advice are seen as taking place where the recipient of the service is based. Dealing in investments can take place in either jurisdiction or both, depending on the circumstances of each transaction.³

4.7 Several conclusions may be drawn from this overview:

- a) there are material differences in what is regulated, how things are regulated and the basis on which specific requirements are triggered;
- b) regulatory protection forms part of the service which consumers purchase when they obtain financial products from an authorised firm;
- c) consumers who buy from an overseas firm are buying some or all of that country's regulatory standards and may well not be covered by some or all of the safeguards applied in their own country; and
- d) it is unlikely that many consumers have the technical knowledge to make an informed choice about which country's regulatory protection they wish to enjoy.

³ The UK would therefore tend not to require a non-EEA overseas fund manager providing services to people in the UK via the Internet to be authorised, because the regulated activity of managing funds does not take place in the UK. In the case of an Internet stockbroker, as long as the stockbroker comes within the so-called overseas persons exclusions then authorisation is not required. To gain the benefit of these exclusions the stockbroker's web-site would have to comply with UK marketing standards, which in this instance would require the site to be issued or approved by a UK authorised firm. If the site contained investment advice, such as a recommendation to buy or sell a share, an authorisation requirement would be triggered, since advice is viewed in the UK as taking place where the recipient of a service is based, again unless an overseas persons exclusion applied.

Q1: Do you agree with this analysis and conclusion?

The FSA's response

- 4.8 The FSA's response to increasing levels of globalisation is based on four principles of action:
- 4.9 **Sophisticated consumers can protect themselves.** The UK's policy is not to impose authorisation or conduct of business (including marketing) requirements on overseas firms marketing or providing services to professional counterparties in the UK, whether that activity is viewed as taking place in the UK or not. This is an application of the FSA's differentiated approach to regulation, in which standards of consumer protection vary according to the sophistication of the consumer. Professional counterparties are presumed to know what they are doing and to be capable of making informed choices.
- 4.10 **Vulnerable consumers need information and protection.** The global reach of e-commerce brings potential risks to consumer protection standards. However, there is at present little evidence that the majority of consumers in the UK are inclined to place their money with financial institutions that are relatively unknown to them. This is what one might expect in a sector in which trust plays such an important role. While the virtual high street may not yet have become a global high street, the FSA is concerned that consumers have access to sufficient information so as to be in a position to exercise informed choice.
- 4.11 Information needs to be clear, fair and not misleading if consumers are to develop sufficient confidence to exploit the global potential of cyberspace. The FSA will, therefore, continue to require firms communicating a financial promotion to UK consumers from non-EEA countries to ensure that their marketing material, including material on web-sites, meets UK standards. (The position as regards firms operating from within the EEA is discussed in Annex B.) The FSA will also need to ensure that information is made available to consumers about the consequences of obtaining financial services from firms that are not authorised in the UK, for example whether or not there is access to compensation or ombudsman schemes (see chapter 8).
- 4.12 **Legal requirements should only be imposed when the FSA's objectives are at risk.** The global nature of cyberspace means that many firms may theoretically be in breach of a number of countries' requirements, merely because a web-site is accessible across the world. The FSA has been concerned to develop a sensible approach to the global nature of the Internet and has sought to reduce the legal risks for firms operating in cyberspace. To this end it took a leading role in conjunction with the Securities and Exchange

Commission (SEC) in developing the ‘directed at’ or ‘targeted at’ test.⁴ This test significantly reduces the risk to firms of having to comply with the requirements of every country in which their web-site is accessible, restricting the exercise of jurisdiction to firms whose sites are targeted at a particular country.

- 4.13 Under the Financial Services and Markets Act 2000 (FiSMA), FSA policy in this area is incorporated into law. As regards non-EEA authorised firms, in order for them to avoid having to comply with UK financial promotion requirements, they must indicate on their web-site that the communication is not directed at UK persons, they must indicate on the web-site that the communication must not be acted on by persons in the UK, they must not refer to the communication in, or make it directly accessible from, any other communication which is made to a person, or directed at persons in the UK; and they must have in place proper systems and procedures to prevent recipients in the UK from doing investment business with them. Compliance with all four of these requirements will give firms a legal safe harbour.
- 4.14 **Global co-operation is necessary to regulate a global medium.** The more firms operate globally and the more consumers obtain financial services internationally, the greater the need for regulators to co-operate, and the greater the benefit of harmonising core standards of regulation and raising standards of supervision across the world. Co-operation takes place on a bi-lateral basis between regulators, and on a multi-lateral basis in fora such as the Basel Committee, International Organisation of Securities Commissions (IOSCO), International Association of Insurance Supervisors (IAIS), and various EU committees. Co-operation covers issues of policy, the supervision of individual firms, the investigation of potential wrongdoing and the taking of enforcement action. It is the FSA’s policy to play a full role in international fora for four reasons:
- a) international fora help disseminate good practice globally and thereby raise standards of supervision;
 - b) in an interconnected world there are likely to be considerable advantages in developing common standards of market integrity and consumer protection, since high standards benefit everyone, and foster a global market-place;
 - c) it is important that the recommendations of international fora do not run counter to the statutory objectives and the four principles of action outlined above ; and

⁴ The ‘targeted at’ or ‘directed at’ test has been widely adopted throughout the world. It was recommended by the International Organisation of Securities Commissions (IOSCO) and has been widely adopted by its members and has also been suggested by the International Association of Insurance Supervisors, and found expression in the EU’s Brussels Regulation governing the circumstances in which the court of the Member State of a consumer has the jurisdiction to try a case.

d) the authority of international fora is undermined if leading regulators feel free to ignore their recommendations.

Q2: Do you think the FSA's policy regarding globalisation and e-commerce strike the right balance in seeking to meet the challenges of this new media? If not, what do you think the FSA should be doing?

4.15 For a summary of the scope of current fora and initiatives in the international arena concerning e-commerce see Annex B.

5 Review of e-commerce risks

- 5.1 The FSA's strategic review, *'New Regulator for a New Millennium'*, laid out an enhanced risk based approach to regulation. Four areas were selected in which a thematic review would be undertaken to identify the risks to the achievement of the FSA's objectives. These risks would then be assessed, prioritised and the appropriate regulatory response determined. One of the areas chosen for such a cross-FSA review was e-commerce.¹
- 5.2 An analysis of the risks presented by e-commerce needs to begin by identifying what it is that makes the Internet that much more than just another communications and delivery channel, and therefore why it is that the Internet commands the kind of attention which has not been enjoyed by other technological advances, such as the fax machine.
- 5.3 The first stage in the review of the FSA's approach to e-commerce was descriptive and analytical, to check there were no important risks to the statutory objectives that were being ignored. The work, therefore, involved:
- a) seeking to identify all significant risks;
 - b) prioritising the risks to determine the most important ones;
 - c) producing an inventory of current and planned actions by the FSA that were designed to address these risks; and
 - d) assessing the adequacy and appropriateness of these actions so as to form a basis for deciding which risks most needed further attention.
- 5.4 The E-Commerce Theme identified over 80 risks of various sorts. These were then prioritised on the basis of the FSA's risk methodology. This involved assessing the likely impact should a risk materialise and the probability of that risk materialising. A risk with a high probability of crystallising, and whose impact would also be considerable, clearly warrants greater attention than a risk which is less likely to happen or which would have a lesser impact.

¹ The E-Commerce Theme carried out the work outlined in this chapter. Also mentioned in this discussion paper is another of the four themes, the Money Laundering Theme, see paragraph 9.28.

- 5.5 Ideally, impact and probability assessments would be based on quantitative data, but in a fast changing market relevant data, even of a proxy sort, is frequently not available, and so the assessments were inevitably of a more judgmental nature. The FSA's Practitioner Forum and Consumer Panel were asked to assess the priority risks that were identified and suggest any omissions. The priority risks and the methodology used to determine them were also discussed with some external third parties.

17 PRIORITY RISKS IDENTIFIED

Box 1

Business risks

- 1. A breakdown of controls related to the development of e-commerce business leads to consumer detriment, failure or significant loss in a firm or firms.**

Ways this risk may materialise: pressure of speed to market leads to control processes being bypassed; management does not understand the risks; key staff leave; a firm is unable to adapt control processes to shorter development lifecycle; a firm has poor policies, standards, and/or control processes; an outsourcing relationship fails; policies, standards, or control processes are not enforced; general project management risks are not controlled.

The FSA's statutory objectives most at risk: Market confidence, Consumer protection, Financial crime

- 2. Problems with an outsourced function, or a heavy dependence on a third party for a material aspect of an e-commerce service leads to consumer detriment, failure or significant loss in a firm or firms.**

Ways this risk may materialise: critical dependence on a software supplier; adverse publicity linked with third party resulting in reputational damage to the firm; a firm's outsource supplier fails to deliver on time and to standard.

The FSA's statutory objectives most at risk: Market confidence, Consumer protection, Financial crime

- 3. Prolonged problems in the availability of firm(s) key e-commerce systems lead to consumer detriment, failure or significant loss in a firm or firms.**

Ways this risk may materialise: external hacking/sabotage; internal sabotage; serious virus problems; serious software problems; serious hardware or network problems; an alliance partner/outsourced service provider fails to deliver a key service; poor crisis management procedures.

The FSA's statutory objectives most at risk: Market confidence, Consumer protection, Financial crime

4. Firm(s)' problems coping with the customer-driven scale of demand lead to consumer detriment, failure or significant loss in a firm or firms.

Ways this risk may materialise: problems with systems; problems with operational processes surrounding key systems; a firm is unable to accurately predict peaks and troughs of demand; failure of contingency planning; poor crisis management.

The FSA's statutory objectives most at risk: Market confidence, Consumer protection

5. Criminals commit fraud using information gathered from consumers' PCs.

Ways this risk may materialise: criminals use malicious software or other means to gather account details or passwords from PCs used by consumers whether in the workplace, at home or elsewhere (the spread of Broadband, or other technologies leading to an 'always on' connection, may increase this risk).

The FSA's statutory objectives most at risk: Market confidence, Consumer protection, Financial crime, Public awareness

6. There is significant financial crime via e-commerce channels.

Ways this risk may materialise: security measures are inadequate to counteract the latest electronic threats; information theft; denial of service attack; a consumer does business with, or gives confidential information to, a spoof web-site; an aggregation service provider uses information illegally.

The FSA's statutory objectives most at risk: Market confidence, Consumer protection, Financial crime, Public awareness

7. Major e-crime or security incident leads to a loss of confidence in the Internet as a medium, and subsequently to major disruption of a market or financial sector.

Ways this risk may materialise: series of major security incidents such as large-scale fraud or theft of confidential information through external hacking; a large number of co-ordinated hacking attacks on financial institutions; criminal attack causes inaccessibility of web-site.

The FSA's statutory objectives most at risk: Market confidence, Consumer protection, Financial crime, Public awareness.

8. Criminal or terrorist attack on payments and settlement systems leads to major disruption and/or financial crime.

Ways this risk may materialise: increased connection of internal networks to external networks making attack easier; security measures are inadequate to control risks; security measures are too outdated to counteract latest electronic threats.

The FSA's statutory objectives most at risk: Market confidence, Consumer protection, Financial crime, Public awareness

9. Consumers suffer detriment as a result of making choices based on false assumptions about the status of information or the quality of firms' analysis of their circumstances, gained via e-commerce delivery channels.

Ways this risk may materialise: firms subject consumers to high pressure selling as result of use of information gathered from PCs; consumers make incorrect assumption that tailored marketing shows assessment of their needs; excessive reliance on web-site content, for example consumers buy without taking financial advice when required; understanding of on-line products is impeded by poor web-site design; a consumer cannot find the information they need from the vast quantity available.

The FSA's statutory objectives most at risk: Consumer protection, Public awareness.

10. Misuse and/or compromise of electronic signatures leads to consumer detriment, failure or significant loss in a firm or firms.

Ways this risk may materialise: consumers believing that they have entered into a contract when in fact they have not; compromise of digital certificate system leads to significant loss in the firm issuing electronic signatures supported by digital certificates or to users relying of them; reliance on electronic signature for purpose for which it is not fit; inappropriate reliance on electronic signatures aids money laundering.

The FSA's statutory objectives most at risk: Market confidence, Consumer protection, Financial crime

Risks arising within the FSA

11. Significant elements of the regulatory requirements and their burden do not work effectively for e-commerce, are missing, or are inconsistent.

Ways this risk may materialise: regulatory requirements are not appropriate for the e-commerce environment; framework of regulatory requirements is not sufficiently flexible to keep pace with developments; regulatory framework is unable to cope with on-line delivery or a new type of financial service or product.

12. The framework of international requirements on e-commerce delivery channels, either agreed or emerging by default, significantly limits the effectiveness with which the FSA can achieve its objectives.

Ways this risk may materialise: unhelpful international regulatory framework emerges; lack of international co-operation, meaning that opportunity to establish a suitable international regulatory framework is lost.

13. There is failure to develop effective supervisory/enforcement techniques for the e-commerce business of authorised firms.

Ways this risk may materialise: compliance with e-commerce requirements is not monitored effectively; the legal perimeter dividing authorised and non-authorised firms is not monitored effectively on-line.

14. An e-commerce related problem is primarily due to inadequate regulatory resources: insufficient resources generally, regulators inadequately informed or trained for their e-commerce, or a lack of staff with special skills.

Ways this risk may materialise: lack of appropriate training for FSA staff; research is not used effectively to identify risks; lack of regulatory resources; lack of IT risk specialists.

15. Regulatory failure occurs due to slowness of response or inability to deal with need to respond to an e-commerce related problem.

Ways this risk may materialise: the FSA's crisis management plan is not adapted to deal with an e-commerce incident; decision making structures are ineffective.

16. Breach of the FSA's site security or incorrect web-site information, leads to a loss of FSA credibility.

Ways this risk may materialise: the FSA's web-site is defaced or altered; loss of integrity of information; loss of availability; loss of confidentiality; web-site is out of date or incorrect due to poor procedures for updating content.

17. The U.K. regulatory framework leads firms to move significant staff or activities overseas (even if still retaining a U.K. presence).

Ways this risk may materialise: it is much easier to move e-commerce business, particularly to elsewhere in the EEA; the FSA fails to provide an appropriate regulatory environment; failure to co-operate effectively with overseas regulators leads to opportunities for regulatory arbitrage.

- 5.6 The 17 priority risks (see Box 1 above) may be divided into two main categories. The first are risks arising within industry, for example :
- a) availability problems with e-commerce systems leading to consumer loss; or
 - b) significant crime via e-commerce delivery channels.
- 5.7 The second category are risks arising within the FSA which, if left unmanaged, could affect the ability of the FSA to meet its statutory objectives, for example the FSA failing to :
- a) adapt its regulatory requirements, techniques, decision making processes to take account of e-commerce;
 - b) recruit sufficient specialist staff; or
 - c) adequately train existing staff to understand the e-commerce environment.

- 5.8 The project team then identified existing work across the FSA that addressed these 17 important risks. In some cases there was a considerable amount of work in train. See Annex A for an outline of existing FSA work.
- 5.9 For some of the other 17 risks, however, significant additional work is needed. This work may be grouped into three areas. These are that:
- a) firms and markets have adequate IT systems and controls to address the risks in their business (see chapter 6);
 - b) consumers have access to relevant and comprehensible information and guidance about obtaining financial services via e-commerce channels; and consumers appreciate that, once armed with this information, they have a responsibility to protect themselves from the risks they can best manage (see chapter 7 and 8); and
 - c) the FSA adapts regulation to e-commerce developments (see chapter 9).

In addition, the FSA needs to ensure that it is well placed to operate effectively and efficiently in an Internet environment (see Annex C).

- 5.10 The following chapters outline the approach which has been developed to mitigate the specific risks identified above.

6 Approach to Information Technology (IT) risk management

E-commerce aspects of IT risk

- 6.1 The use of technology is not new in financial markets. The FSA recognises that many authorised firms¹ have for some time been heavily, if not critically, reliant on their IT systems to process ‘traditional’ products and services. It is often difficult to distinguish between e-commerce IT systems and controls on the one hand, and more general IT systems and controls on the other. In keeping with its policy of technological neutrality, the FSA does not wish to have a special approach to e-commerce IT where this is not justified by differences in risk. Consequently, rather than concentrating solely on e-commerce, this chapter considers the impact of IT in use at firms more generally and what would be an appropriate response by the FSA. These IT risks warrant attention from the FSA as they could impact on the FSA’s statutory objectives and affect firms, consumers and market confidence.
- 6.2 The risks identified in the FSA’s e-commerce review included those associated with availability, capacity, security and financial crime through e-commerce delivery channels. Some examples of the e-commerce aspects of more general IT risks are detailed below :
- a) availability of systems has always been an important issue in firms, but public expectations in the e-commerce environment are 24 hours a day, seven days a week availability and any unplanned ‘downtime’ of systems can be very public and reputationally damaging;
 - b) capacity and ‘stress’ testing are features of any system implementation, but capacity and prediction of demand for e-commerce systems can be more difficult than for internal systems;
 - c) in the area of security, e-commerce opens up firms’ systems to the outside world. While the same underlying security principles apply, the connection

¹ The use of the term ‘firms’ in this chapter should be taken to mean authorised firms and markets regulated by the FSA.

of internal systems and networks to the Internet brings with it different technical means for addressing risks and a need for increased focus on information system (IS) security; and

- d) as identity is easier to disguise in a non-face-to-face environment, there is the potential for the impersonation of *bone fide* customers, identity theft, and hiding suspect transactions (for the purposes of money laundering or other financial crime).

6.3 As already discussed, these risks are not unique to the e-commerce environment. The principles of good IT risk management still apply whenever the use of technology is material to a firm, whether that technology is used for an e-commerce offering or an internal system. The FSA believes that, although the use of e-commerce channels can focus attention on the need for appropriate IT controls, IT risks and the FSA's approach to them are better dealt with by considering IT risk management as a whole. This chapter therefore takes a wider look at the impact of technology and what would be an appropriate response by the FSA.

The FSA's response

- 6.4 Responsibility for achieving adequate IT systems and controls lies with firms and responsibility for setting the control framework lies with senior management.² The FSA recognises that the IT risks firms face will differ, but would expect that the level and types of control are commensurate with the IT risks being run by a particular firm. However, the FSA recognises that it too has a role to play.
- 6.5 In the rest of this chapter four main approaches the FSA could take to help firms achieve this goal of adequate IT risk management are discussed. These are :
- a) ensuring IT risk management is properly considered at a senior level;
 - b) clarifying FSA's expectations in this area;
 - c) incentivising good / adequate IT risk management; and
 - d) helping the dissemination of good practice.
- 6.6 The extent to which the FSA's existing approach in each of these areas adequately addresses the risks is reviewed in the rest of this chapter. Where considered necessary, further possible actions are discussed. In summary, while the FSA is already addressing these risks through the existing

² This accords with the principles of good regulation and the role of senior management. This principle is designed to guard against unnecessary intrusion by the regulator into firms' business and requires the FSA to hold senior management responsible for risk management and controls within firms.

framework of its regulatory approach, this chapter contains some suggestions for strengthening this approach further.

- 6.7 The key proposals are that in the short term the FSA will:
- a) promote senior management awareness of their responsibilities through use of measures such as speeches and circulars to firms' senior management;
 - b) clarify FSA's expectations through the use of measures such as speeches, articles, liaison with industry bodies;
 - c) carry out minor enhancements to the e-commerce questionnaire used in authorisation and supervision; and
 - d) aid the spread of good practice by use of additional measures such as speeches, articles, dissemination of results of peer group reviews.
- 6.8 In the longer term, some measures the FSA could consider include:
- a) adding guidance, in a more explicit manner than at present, on senior management responsibility for adequate IT systems and controls in the High Level Standards of the FSA Handbook (section on senior management arrangements, systems and controls);³
 - b) clarifying FSA's expectations by adding high level guidance (referring wherever possible to existing external standards or good practice guides) in the Business Standards part of the FSA Handbook (i.e. the Integrated Prudential Sourcebook; the Conduct of Business Sourcebook);
 - c) updating as necessary the Regulatory Processes part of the Handbook (Authorisation and Supervision manuals) to reflect better the approach to IT risk; and
 - d) further enhancing the e-commerce / IT questionnaire to reflect feedback from firms and their advisors.
- 6.9 Any new or changed rules or guidance suggested in this chapter would, if taken forward, be subject to formal consultation and the normal process disciplines, including cost benefit analysis. This discussion paper offers an opportunity to comment and help develop FSA thinking.

³ The latest version of the rules and guidance on senior management arrangements and systems and controls can be found at Annex C of the Policy Statement : High Level Standards for Firms and Individuals (February 2001).

Ensuring IT risk management is properly considered at a senior level

- 6.10 **Current position.** The FSA considers that senior management is responsible for putting in place structures in place to manage IT risk. This responsibility is necessary because IT risk is often a significant component of the overall level of risk being run in financial firms. Arguably, lack of familiarity with technology and technology issues differentiates senior management responsibility for IT from senior management responsibility in a number of other areas. Although senior management responsibility for IT risk is implicit in the FSA Handbook, this is an area where the FSA has not made an explicit statement.
- 6.11 **Proposed approach.** In the short term, it is proposed that the FSA develops material, perhaps including briefing for firms' senior management in the form of a circular, to raise awareness of this issue. This will include reference to the FSA's expectations in this area. These expectations may be summarised in the paragraph below:
- Where a firm uses information technology, senior management should have an IT risk management framework that enables controls to address the security, availability and adequacy of that technology. The nature and extent of those controls will depend on a variety of factors, such as the extent of the technological dependency, and could typically include:*
- a) a policy statement setting out the IT risk management framework; and*
 - b) an organisational structure with delegated responsibilities for the implementation of the framework and its related controls.*
- 6.12 In the longer term, one option is to include guidance, in a more explicit manner than at present, on this responsibility in the FSA Handbook as part of the High-level Standards (Senior Management Arrangements, Systems and Controls). This would have the effect of ensuring a continuing emphasis on such responsibility and provide a high level structure for the existing and any future references to IT risk management in the rest of the Handbook.
- 6.13 Principle 3 of FSA's Principles for Businesses⁴ states that a firm must 'take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems'. The current policy statement as part of the High-level Standards (Systems and Controls in Annex C), provides both generic responsibilities across systems and controls, and more detailed rules and guidance that apply to eleven key areas. These eleven areas are:

4 See Annex A of the Policy Statement : High Level Standards for Firms and Individuals (February 2001).

Organisation	Compliance	Risk Assessment
Management Information	Employees and Agents	Audit Committee
Internal Audit	Business Strategy	Remuneration Policies
Business Continuity	Records	

6.14 In none of these eleven areas is there a specific reference to IT. However, IT risk and control is implicit in a number of these areas, for example management information, business continuity, strategy, records and risk assessment. This could be made explicit by adding text to highlight that adequate IT risk management is a significant component in many of these areas.

Q3: Would awareness measures to disseminate FSA's expectations of senior management in this area be helpful? If so what measures would be useful?

Q4: What are your views on making this responsibility more explicit in the High Level Standards in the FSA Handbook?

Clarifying FSA's expectations

6.15 **Current position.** The FSA's constituent bodies had a range of regulatory requirements related to IT systems. The different approaches, in part, reflected the historic use of technology in a particular sector. The FSA considers there should be an assumption in favour of consistency, i.e. any different requirements should reflect a difference in risks.

6.16 Some discussion of risks and clarification of FSA expectations in the area of e-commerce have already been carried out for example:

- a) speeches – during 2000, FSA senior management gave speeches⁵ which had extensive reference to e-commerce and its related risks (<http://www.fsa.gov.uk/pubs/speeches/index-2000.html>); and
- b) press releases – for example the announcement of 'seven principles to help securities regulators face the new global challenges' (<http://www.fsa.gov.uk/pubs/press/2000/>).

However, these do not formally articulate the FSA's expectations in the area of IT risk management.

6.17 The Recognised Investment Exchange (RIE) and Recognised Clearing House (RCH) Sourcebook, the specialist sourcebook covering recognised bodies under Part XVIII of the FiSMA, includes guidance on IT systems and controls

⁵ See, in particular, speeches by Carol Sergeant (29th March 2000) and Howard Davies (19th June 2000).

(see extract in Box 2 below). This reflects the changes from open outcry and the much greater reliance these organisations are placing on information technology.

EXTRACTS FROM THE RIE AND RCH SOURCEBOOK

Box 2

Chapter 2 – Recognition requirements

2.5 Systems and controls

Information technology systems (all guidance)

- 2.5.18 Information technology is likely to be a major component of the systems and controls used by any UK recognised body. In assessing the adequacy of the information technology used by a UK recognised body to perform or support its relevant functions, the FSA may have regard to:
- (1) the organisation, management and resources of the information technology department within the UK recognised body;
 - (2) the arrangements for controlling and documenting the design, development, implementation and use of information technology systems; and
 - (3) the performance, capacity and reliability of information technology systems.
- 2.5.19 The FSA may also have regard to the arrangements for maintaining, recording and enforcing technical and operational standards and specifications for information technology systems, including:
- (1) the procedures for the evaluation and selection of information technology systems;
 - (2) the arrangements for testing information technology systems before live operations;
 - (3) the procedures for problem management and system change;
 - (4) the arrangements to monitor and report system performance, availability and integrity;
 - (5) the arrangements (including spare capacity and access to back-up facilities) made to ensure information technology systems are resilient and not prone to failure;
 - (6) the arrangements made to ensure business continuity in the event that an information technology system does fail;

- (7) the arrangements made to protect information technology systems from damage, tampering, misuse or unauthorised access; and
- (8) the arrangements made to ensure the integrity of data forming part of, or being processed through, information technology systems.

2.5.20 The FSA may have regard to the arrangements made to keep clear and complete audit trails of all uses of information technology systems and to reconcile (where appropriate) the audit trails with equivalent information held by system users and other interested parties.

Chapter 3. - Notification rules for UK recognised bodies

3.16 Information technology systems

Guidance

3.16.1 The purpose of REC 3.16 is to ensure that the FSA receives a copy of the UK recognised body's plans and arrangements for ensuring business continuity if there are major problems with its computer systems. The FSA does not need to be notified of minor revisions to, or updating of, the documents containing a UK recognised body's business continuity plan (for example changes to contact names or telephone numbers).

Rule

3.16.2 Where a UK recognised body changes any of its plans for action in the event of a failure of any of its information technology systems resulting in disruption to the operation of its facilities, it must immediately give the FSA notice of that event and a copy of the new plan.

Rule

3.16.3 Where any reserve information technology system of a UK recognised body fails in such a way that, if the main information technology system of that body were also to fail, it would be unable to operate any of its facilities during its normal hours of operation, that body must immediately give the FSA notice of that event and inform the FSA :

- (1) what action that UK recognised body is taking to restore the operation of the reserve information technology system; and
- (2) when it is expected that the operation of that system will be restored.

Chapter 5 – Applications for recognition (UK recognised bodies)

5.2 Application process

Guidance

5.2.6 Under section 289 (Applications: supplementary), the FSA may require the applicant to provide additional information and may require the applicant to verify any information in any manner. In view of their likely importance for any application, the FSA will normally wish to arrange for its own inspection of an applicant's information technology systems.

- 6.18 **Proposed approach.** In the short term, the FSA could further clarify its expectations through use of information and awareness measures such as speeches, articles and liaison with industry bodies.
- 6.19 For longer term effect, for greater clarity and for a potential safe harbour for firms complying with the guidance, the FSA could revise the Handbook and provide greater consistency and guidance on IT risk. It should be stressed that any such guidance would be high level. For example, it would not specify details, such as encryption levels, but would indicate the principles the FSA expects firms to follow. Nor would any guidance demand inappropriately rigorous standards where the risks do not warrant such an approach. The proposed framework would be intended to provide a baseline so that firms can have a clear understanding of FSA expectations and this would be incorporated into the Business Standards (i.e. the Integrated Prudential Sourcebook and the Conduct of Business Sourcebook).
- 6.20 **Proposed approach – Business Standards, (Integrated) Prudential Sourcebook.** Prudential requirements are currently published in separate sourcebooks, each specific to individual financial sectors, such as insurance or banking. Prudential requirements cover risks that ultimately could threaten the solvency of a firm. In June 2001, the FSA publishes the draft of its integrated sourcebook that will set out harmonised requirements for insurers, deposit takers and investment firms organised by risk category (credit risk, market risk, operational risk, insurance risk and group risk). The implementation date is not yet finalised but could be January 2004. The draft material on operational risk contains material drawing attention to the importance of IT risk, but does not set out detailed requirements or offer guidance on how firms should manage this risk. The FSA will need to revisit the operational risk material when implementing the new approach to capital adequacy for operational risk which is being discussed by the Basel Committee on Banking Supervision and the EU.
- 6.21 Further supporting guidance could be added to the sourcebook, after formal consultation, to cover two main areas:

- a) the IT risks to be considered, how these might give rise to prudential failure and how the firm might address these, including, in due course, through the maintenance of capital resources; and
- b) expectations of adequate practice in the following areas:
 - (i) **information security management.** It is anticipated that extensive reference will be made to the principles of ISO 17799,⁶ the international standard for information security management;
 - (ii) **information system (IS) and IT strategic planning,** to ensure there is an effective link between business objectives and the IS delivery programme, as well as an effective use of technology;
 - (iii) **IT systems programme management,** to keep in focus a firm's business change objectives and to provide a framework by which senior management may direct the change process; and
 - (iv) **IT service management,** to provide high quality computing services aligned to the business needs for availability, security etc.

For areas (ii) – (iv) reference would be made to other relevant good practice guides.

6.22 Outsourcing elements of IT and IT management has been common in institutions for some time, but outsourcing tends to be even more common in the area of e-commerce. Indeed, some aspects of e-commerce outsourcing, for example the type and number of partners, can present particular management challenges. The FSA has already published policy and guidance on general outsourcing by banks. Outsourcing policy will be extended to Building Societies in the Interim Prudential Sourcebook. Requirements applying to a much wider range of firms are included in the draft Integrated Prudential Sourcebook (in the section on operational risk). Again these cover, but do not refer explicitly to, the outsourcing of IT related activities. More explicit reference could be made, if appropriate.

Q5: Would you welcome greater clarity of FSA's expectations regarding IT outsourcing? If so, in what areas?

6.23 **Proposed approach – Business Standards, Conduct of Business Sourcebook (COBS).** The primary purpose of COBS is to set and reinforce business standards for various aspects of a firm's relationship with its customers, typically as an extension of the Prudential Sourcebook controls. Where technology is used as part of that relationship, it is necessary to ensure that the standards are uniformly and consistently implemented.

6 ISO17799 is based on BS7799. BS 7799 / ISO17799 focuses on the desired outcome – making information secure – rather than specifying a particular way in which that outcome is to be achieved. The FSA expects firms to have regard to good practice in guides such as this, but would not require firms to achieve BS7799 / ISO 17799 accreditation.

6.24 Technology has always presented a number of business and consumer opportunities, all with associated risks for which firms need to consider risk mitigation. For example, firms that depend on their telephone system for customer contact may have decided that the postal service is an adequate contingency. However, where contact with customers is via the Internet or e-mail, more sophisticated business continuity plans may be needed to mitigate the risk of prolonged system downtime. Consequently, it is proposed that the current COBS be reviewed to identify what guidance might be introduced. This proposed review might initially focus on:

- a) the security of information gathered from, and held on, customers; and
- b) the availability of services, including additional guidelines on advising customers how to access the service when the firm's computer systems are not working.

Q6: Would you welcome greater clarity of FSA's expectations in the area of IT risk management?

Q7: Would further information / awareness measures be useful?

Q8: Would further guidance in the Prudential and Conduct of Business Sourcebooks be useful? If so, what areas should be focused on?

Incentivising good / adequate IT risk management

6.25 **Current position.** The FSA has already been carrying out work to assess IT risk management in firms and markets. The number of IT related supervisory visits and audit reports commissioned has gone up in recent years, reflecting the increased importance of this risk to firms and in supervision. Consideration of IT risk is now a part of the risk assessment framework which will be used for all financial firms across the FSA. As with all such risks, good risk management on the part of the firm is taken into account in the supervisory process and may result in reduced intensity of supervision. A summary of this work and changes already in progress is outlined below.

6.26 **Current position – firm focused work.** Current work to monitor compliance with adequate standards through firm focused work includes use of :

- a) the IT systems questionnaire;⁷
- b) the detailed e-commerce business and systems questionnaire;⁸

7 This is part of the authorisation pack which is sent to most applicant firms. It addresses a limited number of IT issues and in some cases may need to be signed-off by a firm's external auditors.

8 This is currently distributed as a supplement to the authorisation pack where IT systems are considered to be material to the application. It can also be used for assessing material developments in existing firms including applications by authorised firms that want to add to the regulated activities they are permitted to undertake. Historically the questionnaire was developed as a result of the growing number of financial services being offered over the Internet. Sign off by external IT auditors is usually required.

- c) supervisory team visits;
 - d) internal and external auditors; and
 - e) visits by the FSA's IT risk specialists, supporting authorisation and supervision staff, to focus on IT risk assessment and risk management.
- 6.27 At present, constituent bodies of the FSA can commission reporting accountants to undertake reviews of IT systems and controls (for example section 39 and 41 reports under the Banking Act). Under the FiSMA the FSA has the authority to use 'skilled persons' to assist in meeting its objectives.⁹ This will allow flexibility for the FSA to identify the most appropriate resource for a particular task including IT reviews, to supplement the internal FSA skills and resources.
- 6.28 **Current position – peer group/sectoral visits.** In addition to firm focused work, compliance with adequate practice can also be monitored through peer group and sectoral visits such as reviews by the FSA's IT risk specialists to groups of firms on specific issues. Examples already carried out in the e-commerce field would be the peer group work carried out on Internet controls and business to business e-commerce (see Annex A). This work also helps keep the FSA up-to-date on new developments, and informs future policy work and the FSA's view of good practice.
- 6.29 As part of the FSA's new approach to regulation there is likely to be increased emphasis on peer group or issue based visits. This will be as evident in the area of supervision of e-commerce and IT systems and controls as in other areas of regulation.
- 6.30 **Proposed approach – questionnaires relating to IT and e-commerce.** The FSA has a policy of technological neutrality and will respond appropriately to material IT risks whether or not this risk derives from Internet related technology. The depth of FSA interest in the IT controls of a firm should also reflect the materiality of the IT related risks both to the firm and the FSA's objectives. The FSA is reviewing its current procedures in this area. Some options under consideration are outlined below.
- 6.31 Short term (over next few months) changes might include:
- a) adjustments to the existing IT and e-commerce questionnaires;
 - b) more guidance on the completion of e-commerce questionnaire; and
 - c) consideration of the questionnaire and surrounding processes in the light of the new statutory application timetable for authorisation.

⁹ See consultation paper 91 on 'Reports by skilled persons' (May 2001) for the most recent proposals.

Q9: Are there particular amendments to content or process of the current e-commerce questionnaire that should be considered as part of this short term review?

Q10: Are there other issues or suggestions that should be considered in the short term review?

6.32 Longer term developments could include:

- a) introducing a short initial IT questionnaire;
- b) supplementing this by a more detailed IT questionnaire (incorporating the current e-commerce questionnaire plus any further adjustments); and
- c) structuring the more detailed questionnaire to incorporate mandatory and optional sections to reflect the applicant's business and IT risk profile.¹⁰

Q11: Are there amendments to content or process of the current e-commerce questionnaire that should be considered as part of this longer term review?

Q12: Are there other issues or suggestions that should be considered in the longer term review?

6.33 **Proposed approach – possible enhancements to the Authorisation and Supervision manuals.** The Authorisation and Supervision manuals set out how FSA staff apply the Handbook requirements in the course of authorising applicant firms or supervising authorised ones. These will be kept under review to ensure the manuals' text reflects FSA thinking on risk assessment and management including IT risk. For example, the text relating to the authorisation process could be enhanced to reflect more formally the consideration of IT risks that already takes place.

Dissemination of good practice

6.34 **Current position.** As already mentioned, there have been speeches and press releases which discuss risks and try to disseminate good practice in the area of e-commerce. Some of these cover e-commerce aspects of IT risk. The main good practice reference in the area of e-commerce risk management for electronic banking (but also covering aspects of e-commerce controls and IT risk management more generally) is '*Risk Management Principles for E-Banking*'. This has been drawn up by the Basel Committee on Banking Supervision (<http://www.bis.org>) with input from the FSA and UK banks and building societies.

¹⁰ The enhanced questionnaire would need to avoid being unwieldy, particularly for smaller applicants, and e-commerce specific features would need to be retained where necessary. This could be done through a tiered approach.

6.35 Other work in the area of e-commerce and IT risk controls includes :

- a) description of practices seen in larger financial institutions in managing e-commerce risks (*Euromoney* magazine article, December 2000); and
- b) indirect dissemination via informal discussions with trade bodies etc.

Q13: Has the FSA been doing enough in this area? What additional means, if any, should be used? What areas do you think the FSA should focus on?

7 Approach to consumer security

Introduction

- 7.1 The use of the Internet and other web-enabled technologies to provide financial services moves consumers' security vulnerabilities from the purely physical to the IT environment. In the off-line world debit and credit cards may be intercepted before they are delivered, they may be stolen from people's homes, their details may be recorded fraudulently in stores and duplicates generated. In the on-line world consumers must still pay attention to the physical aspects of security. An intruder may discover passwords written down near a computer, and use them to access an account and withdraw funds.
- 7.2 However due to the Internet, on-line consumers also have to consider IT security. Financial institutions, for their part, must adjust to the reduction in end-to-end security. Firms may control their own systems. Communication between them and their consumers may be encrypted and rendered extremely difficult to decode. But financial institutions have no control over how securely information is protected on their customer's computers, nor on those of third parties, such as retail stores.
- 7.3 The most significant risks on-line consumers face may well remain essentially off-line risks, that is poor physical security and password control, but they are not the only ones. Spoofing,¹ sniffing,² hacking,³ and viruses⁴ do expose an inexperienced public to risks when on-line. Risk management is always harder when the risks themselves may not be understood and the effectiveness of counter-measures difficult to monitor.

1 'Spoofing' refers to an attempt to gain access to a system by posing as an authorised user.

2 'Sniffing' involves the use of a software program that is illicitly inserted somewhere on a network to capture ('sniff') user passwords and other information as they pass through the system.

3 'Hacking' refers to the practice of breaking into a computer without authorisation.

4 A 'virus' is a computer program that can amend code and spread copies of itself without it being obvious. Many viruses also have some sort of 'payload' ranging from jokey messages through to sending confidential information to a stranger, or even to making the whole computer unusable.

7.4 The security risks faced by on-line *financial* consumers are, in many cases, the same as the risks faced by consumers buying *non-financial* products on-line. However, there are some aspects of on-line financial transactions which could affect consumer security in a somewhat different manner than on-line non-financial transactions. The FSA therefore has a role to play, along with others, in making consumers aware of ways to reduce security risks. Some of these differences include:

- a) while both non-financial and financial on-line users face the risk that their credit card details are stolen and the criminal uses the details to make purchases, on-line financial consumers additionally face the risk that their bank account or share account details are stolen. For credit cards, the consumers maximum liability if their card details are stolen and misused is £50.⁵ However, the potential loss that financial consumers face if the security of their bank or share account are compromised may be much larger than this;
- b) the decision to buy a financial product or service may expose the consumer to greater risk than the decision to purchase other goods that are available via the Internet. The purchase of a financial product or service may require disclosure of more information, may involve larger amounts of money, and may have a longer term effect. Consumers conducting financial transactions on-line may therefore require greater security and trust in the on-line financial firm; and
- c) to reduce security risks, on-line financial services tend to have a series of access levels. This means customers have to remember more passwords and private security information to perform financial transactions than when transacting with non-financial on-line firms.

Q14: Are there any other differences that affect the security of on-line financial consumers compared to other non-financial on-line consumers?

7.5 Ultimately, consumers are responsible for keeping financial and other important data secure where it is in their control to do so. But in order to do this they need reliable and comprehensible information on what steps to take. The FSA has an interest in such information being accessible to the public, since it is directly relevant to the statutory objectives of reducing financial crime, protecting consumers and promoting their understanding of the financial system. Information on security will also help consumers form a realistic assessment about the risks involved in on-line financial transactions

⁵ Under sections 83 and 84 of the Consumer Credit Act 1974, the debtor under a credit-token agreement will only be liable to the extent of £50 (or the credit limit if lower) for loss to the creditor arising from the use of the credit-token by another person not acting, or being treated as acting, as the debtor's agent.

and help protect them from unnecessary fears. Total security does not exist in either the off-line or on-line worlds, however adequate security can exist.

- 7.6 Security is, of course, an ongoing challenge both in the physical and on-line worlds. The techniques for committing fraud and measures to reduce risk alter over time, and all those with an interest – police, government, regulators, firms, as well as consumers – will have to continue to meet the challenge. Consumers have always had a role to play. Their responsibility does not change merely because they are operating on-line.

Three IT security risks facing consumers

- 7.7 There are three main security vulnerabilities to which consumers need to attend. See Annex D for more details on all three areas.
- a) The first is that a criminal finds or correctly guesses passwords and other data that are used to log-on to the site of a financial institution and, having gained access to the account, steals money. This risk is mitigated through good password practice.
 - b) The second area of vulnerability is that a criminal sends an e-mail, containing a malicious computer program. Such a program might record the account holder's key strokes, including his or her security and log-on details, and then send the data back to the criminal, enabling the account to be accessed and funds stolen. This risk is reduced through installing and keeping up to date good anti-virus software.
 - c) The third area of vulnerability is that a consumer is directed to a dummy or look-alike site, or falls victim to on-line scams. The consumer may then enter security and log-on data or credit and debit card details, and thereby enable the criminal to access the individual's account or fraudulently use the credit and debit cards to obtain goods or services. To mitigate the risk of on-line scams, consumers should ensure they know the identity of the firm with whom they are planning to do business. They should also confirm that the firm is legal and that it is authorised by the FSA.
- 7.8 Additionally, consumers should try to ensure that the connections between on-line firms and themselves are secure. One way of helping to ensure that the connection is secure is to look for a security icon, usually signalled by an open padlock icon on the screen changing into the locked position.

Q15: Are the security precautions suggested above and in Annex D reasonable and realistic? Are there any other security precautions that consumers should take to safeguard important data?

Consumers' current approach to security

- 7.9 To assess how the public currently addresses Internet security issues, the FSA commissioned the National Statistics Omnibus Survey to investigate consumers' approach to security in cyberspace. Over 1600 people were surveyed in January 2001. The results suggest that 9 per cent of the adult population of Great Britain use the Internet to carry out personal banking, 2 per cent carry out on-line share dealing, 3 per cent use the Internet to shop around for financial products and 5 per cent surf the Internet for information about banking, financial or investment matters.
- 7.10 Nearly 75 per cent of people who bank on-line said they look for one or more pieces of security information; the most important piece of information to consumers seemed to be the padlock, followed by a familiar company or brand name and then a familiar third party logo, such as Which Trader, Trust UK, or Verisign.
- 7.11 The survey also looked at the measures consumers have taken to protect their PCs. The results here are difficult to interpret because, while 76 per cent of private Internet users said they had anti-virus software, it is not clear how regularly they have updated this software. Infrequent updating is likely to be significant among computers bought with anti-virus software already installed, as many PCs currently are. The results of the survey suggested that people who banked on-line were more likely to have some security protection than private Internet users who did not bank on-line. The survey also suggested that people who had been banking on-line for less than six months (16 per cent of on-line banking and share dealers) were less likely to have security precautions in place than people who had banked on-line for a longer period of time.
- 7.12 Some of the survey focused on passwords. One risk is that consumers use the same password for all sites. Some 86 per cent of consumers do use different passwords for accessing on-line accounts at a bank or stockbroker than those they use for accessing other web-sites.
- 7.13 Another risk is that passwords or passnumbers are not memorised but written down or stored on a computer. More than 50 per cent of private users of on-line banks or stockbrokers store their passwords or passnumbers on their computer either at home or at work so that they do not have to type it in every time they log on. Some 83 per cent write their account passwords down.
- 7.14 A further risk is that the passwords are easily guessed. The survey indicated that the proportion of on-line users of bank and share accounts who used private and personal details, or other easily guessed information, as part of their password was 41 per cent.

7.15 As for keeping passwords secret, 12 per cent of those with on-line accounts with banks or brokers have disclosed their password or passnumber to a non-account holder – normally to the account holder’s partner. The survey also suggested that 80 per cent of people who bank on-line have never changed their password. The statistics were used to determine whether some of these customers might have banked for such a short time that one would not have expected them to have changed their password. However, removing these customers made very little overall difference to the results.

Improving consumer security

7.16 Security is a shared endeavour. Financial service firms, the computer industry and regulators all have a role to play. So does the public. The results of the survey indicate that consumers are concerned about security. They also show that more could be done to address fully the risks. Many of the approaches suggested below are common to all three of the risk areas identified above. Those approaches that do not directly bear on what consumers can do are mentioned below but discussed elsewhere in this paper.

7.17 **Promoting good password practice.** There is a significant amount of information publicly available on using passwords sensibly. The British Bankers’ Association (BBA) has published a leaflet entitled ‘*Your money and the Internet: a guide to home banking and Internet shopping*’⁶ which contains a ten point Internet guide. The Banking Code (published jointly by the BBA, the Association for Payment Clearing Services (APACS) and Building Societies Association (BSA)) also contains advice to consumers about password security. Individual financial firms often have sections of their web-sites devoted to questions of security. Other ways in which good password practice might be disseminated include:

- a) providing similar information on the FSA’s web-site;
- b) making such information available through the FSA’s Consumer Helpline or in a fact-sheet; and
- c) providing material for adult learning programmes, citizens advice bureaux, and school curriculum developments on the importance of good password practice.⁷ This could include computer programs that would allow people to test their own knowledge. Such programs could be made available on the web.

7.18 It is possible for financial firms to enforce good password practice. They might, for example, require the password to be changed at certain times. They might install systems that reject passwords which are easy to guess. On the

6 This leaflet can be found on the BBA web site: <http://www.bba.org.uk/consumers/>.

7 Aiming material at children at schools may also indirectly help educate parents on these issues.

other hand, forcing people to choose passwords which are difficult to remember, especially when these accounts are not accessed every day and have to be changed regularly, may increase the risk that a password will be written down – a careful balance needs to be struck.

Q16: Are these approaches to promoting good password practice realistic? Are there any other approaches which should be considered? What measures should firms take to encourage good password practice?

7.19 **Protecting the computer from attack by software programs.** Combating malicious computer programs is not an area which has received as much attention from the financial services sector as good password behaviour. Furthermore, it is an issue that is relevant to the computer industry as a whole. Nonetheless, it is important that consumers are made aware of the risks and what they can do to reduce them. The ways of disseminating good practice, for example by keeping anti-virus software up to date, are similar to those that can be used to promote good password practice: the FSA web-site, the Consumer Helpline, firms' web-sites etc.

7.20 Regulators and the industry will also need to keep the potential scale of such threats under review in order to have effective counter-measures to hand, should they be needed. These measures include steps firms can take to aid consumer security. These may include the use of a mouse rather than the keyboard to enter important log-in details – mouse movements are harder to record than keystrokes – and moving security to devices such as smart cards. To help counter the virus threat, some financial firms are already supplying anti-virus software to their customers.

Q17: Do these approaches to helping consumers combat the risk of malicious programs seem realistic? Are there any other approaches which should be considered? What measures should firms take to enhance consumer security in this area?

7.21 **Avoiding dummy and fraudulent sites as well as those promoting scams.** The main ways in which consumers can be kept informed of what they need to do to protect themselves is through the FSA's web-site, Consumer Helpline, and the other approaches outlined above. However, firms have an interest in tracking down look-alike or dummy sites and taking action against them, whether or not such sites are promoting financial services.

7.22 Firms may also wish to enable their customers to check whether or not the web-site they have accessed is a dummy or look-alike site. One way in which customers can check the authenticity of the site is where a firm has its web-site certified by a reputable certifying agency. By clicking on the certifying agency's logo on the firm's web-site, the consumer is able to confirm the validity of the certificate on the agency's site.

7.23 The regulator also has an interest in ensuring that firms which are communicating a financial promotion to people in the UK are complying with UK requirements. Surveillance of financial sites on the Internet may help identify firms which are flouting UK requirements. Nonetheless, no form of surveillance can be totally effective. There will always be sites which surveillance software fails to identify as suspicious. One way of making it easier for consumers to identify the web-sites of authorised firms would be to require firms to change their web-site address to a top-level or sub-level domain reserved for financial service firms. Instead of having a web-address <http://www.firmname.co.uk>, the address would be <http://www.firmname.fin.uk> or <http://www.firmname.uk.fin>. This .fin concept, which would make it easier for scams to be identified but has other drawbacks, is discussed in greater detail in paragraphs 9.56 – 9.64.

Q18: Are these approaches to helping consumers become aware of the importance of checking the authenticity of a web-site realistic? Are there any other approaches which should be considered?

Q19: What responsibilities do firms and regulators have in this area? Should the FSA encourage firms to conduct surveillance to ensure their site is not being spoofed or should it be left to the firm to protect their commercial interest, reputation and brand name?

8 Approach to information for consumers

Introduction

- 8.1 Promoting public understanding of the financial system is one of the FSA's statutory objectives. Well-informed consumers are also less likely to fall victim to scams and may be less vulnerable to buying unsuitable financial products. On the Internet there has been an explosion of material, most of it free, some of it misleading,¹ but much of a quality, timeliness and sophistication which would previously have been available only to professional firms, or, in some instances, the larger investment banks.
- 8.2 The availability of material, however, is only part of the story. Any discussion about information and its uses by consumers is necessarily informed by a view of how consumers do understand and misunderstand the information they read, how they behave in e-commerce environments, how they assess risk and their appetite for it, and so on. At present there is very little knowledge of what generalisations may be sensibly made about the average consumer using on-line channels to access financial services. Printed in Box 3 is a set of generalisations drawn from two sources: a literature review commissioned by the FSA and a review by the FSA of research conducted by firms.²

1 For example, care is needed by those who think of trading on unconfirmed reports such as those posted onto investment bulletin boards and chat fora, since these stories may be rumors designed to manipulate markets (see paragraphs 8.35 - 8.41 below).

2 These generalisations are examples of the broad assumptions that may be made in policy making. They are likely to be refined in light of further work.

CONSUMER RESEARCH GENERALISATIONS

Box 3

- It is no longer just the technologically sophisticated or affluent consumer who has access to e-commerce or is buying on-line.
- There is not a correlation between the consumer's technological sophistication and their financial sophistication.
- Consumers are not using e-commerce media in isolation from other information sources and influences, regardless of the delivery channel used to make a purchase.
- Time and experience are needed for people to adjust their behaviour to new risks, whether these risks are brought about by products or communication and delivery channels.
- Research suggests that consumers make many of their financial decisions on the basis of other people's recommendations without being in a position to assess their competence or motives, whether given face-to-face or anonymously via a bulletin board.
- Many consumers do not identify the difference between independent and tied advice. Some do not differentiate between information, informal advice (for example from friends and family) and investment advice in making their investment decisions. Research also suggests that consumers are drawn towards information that appears to be personalised, something which is easy to do on the Internet.
- Consumers tend to be cautious about obtaining services from unfamiliar names;
- New users of new technologies are likely to be most exposed to technology related risks. Teething troubles might include:
 - ordering a product or service twice when only once was intended;
 - not knowing how to navigate round a web-site and thereby missing important information;
 - not understanding how to minimise security risks on-line; and
 - not realising that an agreement may be binding even though a written document has not been physically signed.

Q20: Are there any other characteristics of consumers which are relevant to this discussion paper?

- 8.3 Whatever view is taken of consumer responses to e-commerce, three characteristics of the Internet³ – globalisation, access to vast quantities of data and the development of smart systems to identify and select information and other services – together create a new paradigm in the retail market. This paradigm is marked by the control individuals are given to view material which others have placed on web-servers around the world and the ability of firms to market their promotions (and potentially their pricing) on a far more individualised basis. It is this shift towards greater individual control and individualised targeting which distinguishes e-commerce channels from previous revolutions in mass communications, such as newspapers or television.
- 8.4 Within this new set of market possibilities there are risks as well as opportunities for consumers. The opportunities include greater information, greater choice, greater competition, better value for money and the increased likelihood of purchasing suitable products due to greater transparency and perhaps the use of intelligent agents. It is important not to lose sight of these opportunities. However, they will not be discussed further in this paper.
- 8.5 The focus of this chapter is on the risks faced by consumers. These are generally not specific to e-commerce. For example, the range of information available through e-commerce channels highlights risks arising from how consumers interpret and use information which is available: consumers might be misled in their financial decision making if they relied on highly tailored marketing material which was perceived as providing advice on the suitability of a product; or they might be misled by ‘advertorial’ which looked independent but which, in fact, was a paid for promotion masquerading as a news feature; or they might be misled because poor design impeded their understanding of a product or service. Each of these risks could materialise in the on-line or off-line world, although the probability of the risk arising, and the specific way in which such risks did arise, may vary depending on the channel used.
- 8.6 For this reason, it is not appropriate for the FSA to set out a strategy for consumer information which is specific to e-commerce. Instead, and in line with the policy on technological neutrality, the e-commerce environment will need to be considered in the context of an overall consumer information strategy. Responses to this chapter will, therefore, contribute to existing FSA projects, including work on the disclosure of regulatory status, work on product disclosure and on comparative product information.

3 By using the term Internet, WAP, iTV etc. are also considered. However, the FSA is concentrating on the Internet in this chapter because it is by far the most widely used channel. The National Omnibus survey figures show that, by January 2001, 98 per cent of individuals who used the Internet for personal use had done so using a computer. In contrast, only 7 per cent of adults had done so using a phone, and approximately 6 per cent using digital TV.

- 8.7 The remainder of this chapter will explore the risks in the financial services sector faced by consumers and discuss possible responses to them. Not all these risks are primarily for the FSA to address. In many areas government, industry, educational, consumer or media organisations will have an equally important role to play. The risks may for convenience be grouped into six categories. These are:
- a) **ignoring cyberspace** – the risk that consumers lose out on opportunities because they do not use e-commerce channels;
 - b) **global buying** – the risk that consumers fail to understand the consequences of obtaining financial services from firms operating from other countries, and are more likely to buy from overseas based firms than at present because the Internet makes it easier to do so;
 - c) **information and choice** – the risk that on-line consumers make poor judgements about what to buy, because of the way in which information is disclosed to them;
 - d) **consumer understanding** – the risk that on-line consumers make poor judgements about what to buy, because they do not understand the material they do find;
 - e) **best buys and good decision making** – the risk that on-line consumers make poor judgements about what to buy, because they do not know about, or cannot find, sites which provide objective comparable data on financial products; and
 - f) **scams and crime** – the risk that on-line consumers fall victim to scams and fail to safeguard important information on their computers. This was discussed in the previous chapter.

Q21: Are the risks identified here material and realistic? Are there any material and realistic risks which have not been identified?

Ignoring cyberspace

- 8.8 There is a risk that consumers might ignore the opportunities of e-commerce either through lack of access to equipment or the confidence to use it. The issue of access to equipment is largely for the government to address at a national level. Individual firms which choose to operate on-line will also have an interest in promoting confidence in e-commerce channels. The previous chapter, in conjunction with Annex D, provides advice on how consumers might mitigate the risks of obtaining services on-line. This may be useful in helping individuals form an accurate assessment of the security risks so that they are in a position to make an informed choice about whether or not to use an e-commerce channel. The question is not only the nature of the risk, but

also whether a consumer's decision is informed by a mistaken assessment of risk and reward, i.e. it may be rational for a person who is totally risk averse not to send credit card details over the Internet, whereas it might be not be rational for someone with a higher tolerance of risk to choose not to do so if it meant forgoing a benefit that was of value to him or her.

Q22: Should the FSA be doing anything more to address the risk that consumers might ignore the opportunities of cyberspace?

Global buying

- 8.9 Few consumers enter into a financial relationship with a firm expecting it to go wrong. On the other hand, if things do go wrong, the ease with which redress is available does make a considerable difference. The average consumer in the UK may not realise that by entering into a financial relationship with a firm operating from another country he or she may not be covered by a considerable amount of UK consumer protection, including the UK's compensation and ombudsman schemes. Whether or not there are ombudsman and compensation schemes in the firm's country, which currencies they cover, whether they cover non-residents, whether they cover the same services, what level of redress or compensation they provide and how easy they are to access are all likely to vary.
- 8.10 The Internet has not created the possibility of consumers obtaining financial services from overseas firms, since the phone, fax and mail offer this capability. However, the Internet does increase the ease and therefore the probability of consumers obtaining financial services from firms based in other jurisdictions. Consumers need to be aware that the level of protection in some countries is greater than in others. For example, dealing with a firm authorised in another EU Member State with redress and compensation arrangements comparable to the UK's would be very different from dealing with an unauthorised firm, or a firm from a jurisdiction outside the EU with a minimal compensation scheme. Prior to parting with his or her cash the cautious consumer will need to know that there are questions to ask and how to find the answers.
- 8.11 There are other questions which may arise where consumers seek to compare products marketed in different countries. For example, it may not be clear when comparing collective investment schemes from different countries, (such as a unit trusts or open-ended investment companies (OEICs)) that information on charges may be drawn up on different bases. Tax treatment, national accounting and disclosure requirements in this area may differ.
- 8.12 The intensity with which regulatory standards are enforced will also have an effect on the likelihood of things going wrong, as well as on the ease with

which they are subsequently put right. While such standards may well be broadly equivalent among some countries,⁴ even there they are unlikely to be exactly the same. Consumers will not be able to rely on local disclosure requirements to obtain a full picture, since some things, such as the frequency and method of monitoring, are regulatory practices about which informed judgements are difficult to make.

- 8.13 Furthermore, should a dispute arise which cannot be settled amicably, litigation may be required, and the consumer may find that the contract with the firm is governed by the law of another country and that legal action can be taken only in that country's courts. Obtaining expert advice on another country's laws and regulatory requirements is likely to be expensive and inconvenient, especially where there is a language barrier to surmount.
- 8.14 Where an overseas non-European Economic Area (non-EEA) firm is targeting its financial promotion to people in the UK, its web-site will have to comply with UK requirements. In the case of web-sites promoting investments, the material will either have to be issued or approved by a UK authorised person, and that person is then responsible for the fact that the promotional material is clear, fair and not misleading. In the case of deposit taking and general insurance, specific information must be disclosed, including the firm's name, its country, its regulatory status, the name of any applicable redress or compensation scheme and, for deposit taking, its capital. Where an overseas non-EEA site is not targeting people in the UK, it does not have to comply with these requirements.⁵
- 8.15 The FSA has a duty to provide the appropriate degree of consumer protection and to promote consumers' awareness of the UK's financial system. It does not have a duty to encourage or discourage consumers from obtaining services from overseas firms. Nor does it have the resources or remit to provide advice about the regulatory and legal protections available in other countries. Consumers who do choose to obtain financial services abroad, nonetheless, need to realise that such a choice has consequences which should be carefully considered.
- 8.16 To address the risk that consumers might not realise the extent to which they are contracting out of UK consumer protection, the FSA will need to consider what information to provide. Options include extending the consumer pages of the FSA web-site to provide links to the relevant regulatory sections of the web-sites of overseas regulators, and identifying a set of issues to which consumers might wish to take into account. Such issues might include regulatory requirements, jurisdiction, applicable law, as well as access to compensation and alternative dispute resolution schemes.⁶

4 For example, within the European Economic Area (EEA) where the Single Market Directives create a common set of minimum requirements for financial service firms.

5 The position regarding EEA firms is described in Annex B.

6 For a brief outline of EU initiatives in this area, please see Annex B.

Q23: Should the FSA alert consumers to the importance of considering the significance of potentially different levels of consumer, regulatory and legal protections available overseas? How effective do you think the options suggested would be? Should it be providing other sorts of information, or taking other kinds of steps to address the risk that consumers may not be aware of the consequences of obtaining services from firms based in other countries? How might the FSA do this?

Q24: Aside from differences relating to ombudsman and compensation schemes, regulatory (including accounting) standards, tax and the jurisdiction of courts and the law which they apply, are there any other regulatory or legal differences of a material nature about which consumers need to be aware?

Information and choice

- 8.17 Effective disclosure is one of the foundations for efficient markets. It promotes competition, allows consumers to make informed choices, and exposes wrongdoing. Even where an individual consumer does not actually read the information that has to be disclosed, others in the market do (advisers, analysts, commentators, consumer bodies) and this will, albeit indirectly, tend to influence choice. However, it would be mistaken to conclude that merely because large quantities of information are available in cyberspace, competition across all financial services is equally affected by the Internet. There are grounds for thinking that the Internet makes disclosure more effective in some markets than others.
- 8.18 **Regulated markets.** The rules on listing and post trade disclosure are part of a package of transparency measures which are designed to promote high standards of market integrity. The effect of the Internet is likely to increase the speed with which price determining information is made available to the market and improve the access of all market participants, including retail customers, to it.
- 8.19 **Market for the less complex financial services** (*such as deposit taking or general insurance services*). The FSA does not impose particular disclosure requirements here, since the information is reasonably easy to understand, and consumers can, and in some cases do, switch supplier in order to obtain the service they want at the price they are willing to pay. The Internet makes it easier to identify good value on-line and off-line products, though for consumers significant benefits lie in the fact that product providers are in some areas competing very strongly for their on-line business.

- 8.20 **Market for complex packaged products** (*such as unit trusts and unit-linked life policies, whose details and operation may not be easy to understand*). The impact which the Internet is having in this sector may be considered from two angles. The first is charges, the second is the suitability of consumer choice. As regards charges, the Internet has encouraged an expansion in discount brokers offering unit trusts or OEICS with some or all of the initial fee discounted; there is less price competition on the annual charge that is paid to the intermediary. Many discount brokers now operate via the Internet.
- 8.21 However, competition between intermediaries over the discount on the initial charge is quite distinct from the question of whether the market works efficiently when consumers come to select between the discounted funds on offer. There are grounds for thinking that the Internet has not made much difference in this area. Research commissioned by the FSA⁷ has shown that where products are complex, consumers do not behave in ways that might theoretically be expected. They do not generally research what is available and then make a choice. Indeed, most people do not read about the details of the product they have bought, even though this contains important data on its key features, such as charges and their projected impact on performance.
- 8.22 As regards the impact of the Internet, there is no evidence that it has made the public more likely to read disclosure documents on-line, nor feel any less confused having done so. One might draw a conclusion that many consumers do not know what a rational basis for making an investment decision would be. If true, this would further explain why the minority of people who do read a product's key features, report that they feel overloaded with data they cannot make sense of. On the basis of this research one might expect the large amount of information available over the Internet to have a limited impact on the suitability of the choices consumers make.
- 8.23 The FSA is currently reviewing disclosure requirements for packaged products⁸ to address the market failure alluded to above, and is also reviewing the use of past performance in advertising. Whether or not there should be changes in the quality of the information to be disclosed to consumers will not be discussed here, since this question affects all communication channels, not just e-commerce ones. However, in developing its policy, the FSA will need to bear in mind that the Internet and other web-enabled technologies do have distinct features and that these vary depending on the device used, for example PCs, mobile phones, interactive digital television. Those features which distinguish the on-line from the off-line world include:

7 *'Informing Consumers: a review of product information at the point of sale'* (November 2000). This review can be found on the FSA's web-site at <http://www.fsa.gov.uk/pubs/discussion/04/index.html>.

8 The term 'packaged product' is used to mean a life policy, a unit in a regulated collective investment scheme or an investment trust savings scheme, whether or not held in a PEP or an ISA.

- a) the limited patience of consumers,⁹ especially when they have to wait for large files, such as pictures or PDF files,¹⁰ to be sent across the web;
- b) the attention span of consumers when on-line, which can be short;
- c) the difficulty experienced by many people in concentrating on dense material presented on a computer screen, exacerbated by the inability to print out relevant material for reading off-line from devices such as interactive digital television and WAP;
- d) the way text may be organised on-screen encourages material to be in small, digestible chunks, and permits consumer interaction, for example through the use of decision-trees;
- e) the limited amount of information that can be easily presented on mobile phones, Personal Digital Assistants (PDAs) and hand-held computers;
- f) the poor resolution of television screens compared to those of computers in showing text;
- g) the potential difficulty for the consumer in identifying how to keep a permanent record of information received, for example, on a TV set; and
- h) the use of cookies¹¹ and possibly aggregation¹² to allow firms to target their marketing material with greater accuracy. The impression of personal knowledge of the individual might lead a consumer to believe that he or she was being advised to buy a product which was, in fact, unsuitable for his or her circumstances.

Q25: Are there any other features which distinguish the Internet and other web-enabled technologies and which would need be taken into account when considering what information should be made available to consumers?

- 8.24 There are two sets of implications which may be drawn from the different features of the Internet. The first, which is a commercial matter, is that firms which want consumers to re-visit their site and obtain services are likely to be those which offer superior site design and speed of access, so that consumers who lack cutting edge technology, which provides faster transfer of data, can find what they want without delay.
- 8.25 The second set of implications is that the particular features of certain communication channels may call for specific guidance on how to implement regulatory requirements.

9 Consumers may also be influenced by the cost of being on-line for long periods of time for some e-commerce delivery channels.

10 Portable Document Format file.

11 A cookie is a small amount of textual information about a user that is stored by the browser on a user's PC and can be used to present customised web pages or information.

12 See paragraphs 9.2 - 9.15 for a discussion on aggregation.

8.26 For example, web-enabled devices with small screens, such as those on most mobile phones, are not designed for long documents, such as contract terms or key features documents. Such limitations may not matter where mobile phones are used as part of the selling process, or in the operation of an account once it has been opened, but would raise a number of questions if a firm were proposing to open an account or sell packaged products solely through this channel. These questions include:

- a) is it right for a consumer to be able to buy a product without the firm knowing it has given the consumer access to details of the product and contract in question?
- b) would it be sufficient for a consumer to indicate that he or she had already obtained the product and contract details via some other channel or that he or she did not want to read them?
- c) should any contract be subject to subsequent confirmation, once full details have been provided?
- d) should cooling off procedures be changed for purchases of packaged products? For example consumers might receive a strongly worded statement to the effect that they may have bought the product without reading about its details, that they should now read the key features document and then decide whether or not to cancel.

Q26: Do you think additional guidance is needed concerning the use of small screens, such as those on mobile phones? What do you see as the advantages and disadvantages of the approach put forward above?

Consumer understanding

8.27 The more consumers are able to understand the information available, the more likely it is that they will make better decisions. The FSA has a role to play in promoting consumer understanding, and has its own consumer focused web-site, Consumer Help (<http://www.fsa.gov.uk/consumer/>), which provides a range of information to help consumers make financial decisions. Following the FSA's assessment of the above issues, and that of consumer security, some key messages to consumers will be published in June 2001 (see Annex D). These will be updated in the light of responses to this paper and future market developments.

Q27: What other key messages to consumers should be considered?

8.28 The FSA is not the only body providing information to customers which could help their understanding and reduce the risks with which the FSA is concerned. Government, adult learning colleges, citizens advice bureaux, trade unions, consumer organisations, schools, as well as the financial services industry, all have a valuable contribution to make. The FSA would like to receive views on two specific ways in which consumer understanding of information could be aided. These are:

- a) hyperlinks to and from the FSA's web-site; and
- b) investment bulletin boards.

8.29 **Hyperlinks to the FSA's web-site.** Hyperlinks to the FSA's web-site may be used to address two discrete risks. First, such links would help spread the general message that the FSA exists and that consumers should check with the FSA's Central Register that the firm they are dealing with is authorised.

8.30 Second, a hyperlink to the FSA's site may help address the risk that consumers use e-commerce delivery channels but fail to take full advantage of e-commerce. This may arise because people do not know about or fail to find sites which provide clear and objective data on financial products. Access to the FSA site would also put them in touch with current topical financial issues, such as details of the review into the sale of endowment mortgages.

Q28: Are there any other valuable benefits which consumers may derive from hyperlinks to the FSA's web-site?

8.31 While hyperlinks to the FSA are a cheap and convenient way of putting people in touch with sources of objective data, they would have the potential to mislead if consumers were given reason to believe that the FSA endorsed or recommended a firm or that the firm's web-site was secure. It is possible that the mere presence of a link from a third party to the FSA's site would encourage a customer to think the firm was authorised and a member of the compensation scheme, when in fact the firm may not be. Consumers need to appreciate that the FSA would not necessarily be immediately aware that a third party had linked to its site, and that the presence of a hyperlink says nothing about the status or viability of the firm that establishes that link.

8.32 Firms will also be aware that the Conduct of Business Sourcebook provides guidance for investment firms on hyperlinks (3.14.5 G, page 68 Annex E):

'The FSA's web site <http://www.fsa.gov.uk> contains a wide range of information including pages of specific relevance to customers. Firms may, if they wish, include a reference or hyperlink to the FSA's site; this will not however replace any requirement of the financial promotion rules.'

8.33 The FSA is considering its policy on hyperlinks in the context of the review into status disclosure. In the interim, firms should appreciate that the FSA is happy for them to link to the FSA web-site provided:

- a) the link will not be accompanied by any implication that the FSA endorses or recommends the web-site from which the link originates;
- b) the link will be accompanied by the following statement:

'General information about financial services is available from the Financial Services Authority (FSA). The FSA is an independent watchdog set up by the government to regulate financial services and protect your rights. It provides free and independent information about financial matters on its web-site at: <http://www.fsa.gov.uk/consumer>.'

Q29: Does the policy on hyperlinks seem reasonable?

8.34 **Hyperlinks from the FSA's web-site.** The FSA has, in the past, with limited exceptions, provided hyperlinks only to the web-sites of other public authorities, trade associations and regulatory agencies.¹³ Links to voluntary organisations are considered on a case by case basis. The FSA will be including live links to product providers from the product summary information that will be contained alongside its comparative tables on the launch of this service later this year. Consumers will be taken out of the FSA site via an exit page which will state that they are leaving the safety of the FSA site. It is likely that further guidance will be provided once the tables are issued, such as a statement to clarify that hyperlinks are not a recommendation to buy. The FSA could also consider establishing links from the FSA's Central Register to the web-site of the authorised firm.

Q30: Should the FSA's Central Register of authorised firms contain the firm's web-address? Should the Central Register also have hyperlinks to the web-site of an authorised firm? If so, please give your reasons and say whether or not this link should be to its home page?

8.35 **Bulletin boards and chat fora.** Investment bulletin boards provide a forum in which the public can pass on their views of particular shares, financial products and financial service firms. While bulletin boards and chat fora have a valuable educational function, they have also been widely used in this country and abroad to spread false stories about firms in the expectation of profiting from the false market that is thereby created in the company's

13 Some external sites to which the FSA links include the Financial Services Central Register, the Financial Service Consumer Panel, the Financial Services and Markets Act, HM Treasury, Forum of European Securities Commission, International Organisation of Securities Commission, Australian Securities and Investments Commission, Commodity Futures Trading Commission, Security and Exchange Commission, European Commission, Basel Committee on Banking Supervision. One commercial site to which the FSA has established a link is that of Equitable Life. This was established to enable customers of Equitable who did not know its web-address to keep up to date with events at the life company.

shares. Those engaged in abusive practices may be committing a criminal offence under the insider dealing or market manipulation legislation. They may also expose themselves to enforcement action under the civil fines regime designed to combat market abuse.

- 8.36 In the UK operating a bulletin board is not a regulated activity. Contributors to bulletin boards may be providing investment advice and communicating a financial promotion, but so long as they are not doing so in the course of business, they will not need to comply with requirements relating to these activities.
- 8.37 Bulletin boards, chat fora and those who use them are subject only to self-regulation.¹⁴ Some firms offering this service may however be regulated for other activities. Self-regulation in this area can be effective where those who use a particular service are aware that there may be different standards applied by operators of bulletin boards and where they can therefore decide which boards to visit on the basis of an informed choice. For example, consumers might wish to receive explicit warning by operators of bulletin boards about the risks of relying on unsubstantiated material, or they might be interested to know how frequently operators of bulletin boards monitor material posted there. Disclosure of such information would enable consumers to decide whether they wanted to read material on a bulletin board that operated to a particular set of standards.
- 8.38 The questions arise as to whether there is sufficient awareness within the market of the standards applied by individual bulletin boards, whether a particular standard is reasonable, and if there is a lack of information in this area, what role, if any, the FSA might have, beyond conducting surveillance of bulletin boards, to identify possible attempts to abuse regulated markets.
- Q31: Do you believe that UK users of bulletin boards understand the status of information posted onto different discussion sites? Why do you hold this view?
- Q32: Do you believe that UK users of bulletin boards understand the different approaches followed by operators of bulletin boards? Why do you hold this view?
- 8.39 If consumers are not sufficiently aware of the standards being followed on bulletin boards, the question arises as to whether the FSA should consider drawing up a code of good practice for operators of bulletin boards. Such a code would have the disadvantage that it could be ignored by non-authorised firms. Only in respect of authorised firms operating a bulletin board could the FSA require either compliance with any such code or prominent disclosure that there was or was not compliance with such a code.

14 If contributors to bulletin boards or chat fora were communicating a financial promotion or providing investment advice in the course of business, regulation would apply.

Q33: Would drawing up a code of practice provide any additional benefit to users of bulletin boards? Since non-authorized firms operating bulletin boards would be free to ignore a code of practice, how much benefit would a voluntary code have? Might users of a bulletin board that complied with such a code place too much reliance on material posted there?

Q34: Should compliance with such a code be a necessary requirement for authorized firms operating bulletin boards? Should authorized firms operating bulletin boards be required to disclose prominently on their site whether or not they comply with any such code?

Q35: Should all firms (those authorized and not) be free to monitor their own stated compliance with any such code, or should there be provision for regular third party audit as a condition of being able to say that such a code is adhered to?

8.40 Were a code likely to be beneficial and cost-effective, the question would arise as to what the content of any such code might be. Such a code could be based on the criteria identified by the International Organisation of Security Commissions (IOSCO).¹⁵ These criteria are shown in Box 4.

Box 4

CRITERIA IDENTIFIED BY IOSCO REGARDING BULLETIN BOARDS

Disclosure to those viewing postings

- a warning on the bulletin board that neither the operators of the bulletin board nor persons making postings are authorized to give investment advice;
- a warning that persons viewing postings should consider consulting an authorized firm before investing in a security discussed at the site; and
- encouragement to contact the regulator if a person viewing postings suspects that any posting is inaccurate or based on inside information or likely to mislead or deceive viewers.

Disclosure to those making postings

- a notice that those posting material are personally responsible for the authenticity and accuracy of their postings; and
- a notice that those posting material are expected to disclose any vested interest in a security about which they post.

¹⁵ Report on 'Securities Activity on the Internet II', IOSCO, 2001.

Duties on operators of bulletin boards

- a requirement that operators of bulletin boards monitor discussion sites for misleading or deceptive postings or postings likely to be part of a scheme to defraud investors or manipulate the market;
- a requirement that operators withdraw immediately the rights of access of a person making postings of the kind described above;
- a requirement that operators notify the regulator within a reasonable time of any suspicious posting, complaints about suspicious postings and the identity of persons responsible for such postings;
- a requirement that operators establish the identity of those making postings; and
- a requirement that operators archive and maintain postings for a certain period of time.

Q36: Would a code based around such criteria improve public awareness and reduce the likelihood of misleading postings being made?

Q37: How onerous would compliance with such criteria be (please give details)?

Q38: Since operators of bulletin boards could voluntarily adopt the IOSCO criteria, what benefit would be gained by the FSA issuing a code of good practice?

Q39: Are there any other ways in which operators of bulletin boards might minimise the potential for their sites to be used to abuse regulated markets?

8.41 IOSCO has identified four other ways in which consumers may be protected from misleading material posted onto bulletin boards and similar fora. These are:

- a) subjecting operators of bulletin boards to regulation;
- b) subjecting operators of bulletin boards to mandatory compliance with the criteria mentioned in Box 4, above;
- c) surveillance and enforcement to detect, punish and deter wrong-doing; and
- d) consumer education.

Q40: What are the advantages and disadvantages of these approaches? Do you favour a strategy that is built around particular approaches? If so, which ones and why?

Best buys and good decision making

- 8.42 The Internet provides access to enormous amounts of information, but without the tools to identify information that is wanted from that which is not, the medium would have limited use. Consumers can always track data down on a firm's web-site, but using the Internet simply as a large brochure warehouse is likely to be as hard, and certainly no cheaper, than ordering product information by phone.
- 8.43 What turns the Internet into more than just a virtual high street are the providers of independent data on firms and products, and software programs that sort and compare products. It is these comparative programs which are likely to optimise the impact of disclosure, and these programs, like any comparative tool, are sensitive to the nature and complexity of a product. The more straightforward a product, the simpler it is to produce a software program that will compare the price of an essentially homogenised commodity.
- 8.44 Conversely, the more complex the product, the harder comparisons become. Ranking interest rates available to depositors is a very much easier task than producing a comparative table for fixed rate mortgages with tapered repayments and specific periods when reduced or zero penalties are incurred for switching. It would be harder still to compare products with different risk profiles, for example fixed and variable rate mortgages. And some aspects of a service, for example a mortgage provider's policy on repossession, may be very relevant to some people, but be overlooked in comparative tables.
- 8.45 Furthermore, some services may seem straightforward, but give potentially misleading results if important variables are excluded. For example, the cost of share trading may comprise an annual fee, as well as a charge for each transaction, and the dealing charge may vary depending on its value. The trading cost, however, is only one dimension, since speed of execution and the price obtained are likely to be no less, and probably far more, important. Aggregating these different components into a single table is likely to be difficult.
- 8.46 No less difficult are packaged products, such as unit trusts, pension plans, and with profits life policies. The Internet can be readily used to discover which intermediary firm is offering the best discount on a particular investment product. It may be much harder to rank competing products against each other. It is in response to this complexity that the FSA is preparing comparative information tables. However, the FSA's tables will not recommend any particular product but simply provide data under a number of criteria to enable consumers to make their own comparisons. 'Best buy' programs from other sources may, for example, rank products or identify a

‘top 5’. While ‘best buy’ programs have the potential to be a valuable tool, it is important that consumers recognise their limitations:

- a) they may not interrogate the whole market, but only major brands, and if such a program looked similar to one which interrogated a wider range of products, consumers could easily be misled;
- b) there may be a flaw in the program – the more complex the product area the harder it will be to avoid software error;
- c) an important aspect of a service may not be considered by the program;
- d) there may be a lack of clarity as to what criteria are used to determine a ‘best buy’;
- e) the program may present a favoured brand or brands, rather than the ‘best buy’, at the top of a list; and
- f) a ‘best buy’ says nothing about whether the product is suitable for someone’s individual circumstances.

8.47 In addition to programs that seek to identify a ‘best buy’, there are also software packages that will help consumers decide whether a particular product is suitable for their circumstances. It is important for firms to be aware that identifying best buys for consumers and helping them decide on whether a product is suitable may trigger an authorisation requirement. Authorisation is required where firms provide advice about a particular investment. A best buy program may also be subject to the financial promotion rules, and any arrangements with an authorised firm, for example, to buy an investment product from the provider highlighted by the software might also trigger an authorisation requirement. Non-authorised firms, and authorised firms which are not permitted to provide investment advice, or arrange deals in investments, would be well advised to seek expert legal advice if they have any doubt as to whether ‘best buy’ or ‘suitability’ programs available on their site trigger regulatory requirements.

Q41: Does the FSA need to take any action to ensure that consumers make appropriate use of ‘best buy’ programs?

Q42: Is there any uncertainty over the dividing line between computer programs that facilitate the decision making process (and which are not subject to regulation) and those which provide advice (and which trigger an authorisation requirement)? If so, what are the products or situations which create that uncertainty? Are there any other situations in which the distinction between information and advice may be unclear?

The FSA's response

- 8.48 The FSA has taken two substantial initiatives to help consumers enhance their capacity to make informed decisions. In addition to the comparative information tables, referred to in paragraph 8.46, it has also developed structured decision trees to help consumers decide whether a stakeholder pension is right for them. These decision trees, which will be available on-line, have been subject to extensive consumer research to ensure that the public correctly views them as providing a set of structured questions, rather than investment advice.

9 Adapting the regulatory approach

- 9.1 This chapter examines three areas where the regulatory approach may need to adapt to new e-commerce developments: aggregation, electronic signatures and top level domain names for web-sites. The depth of the analysis varies according to the complexity of the issues involved. The approach, however, is a consistent one: to analyse the nature of the risks to the FSA's objectives and to indicate a range of interventions or approaches that may address these risks.

Aggregation

- 9.2 Aggregation is a service that allows customers to view their on-line accounts and other information held with different institutions at a single location on the Internet. This means that customers can create a single page updated regularly which contains all their financial account statements, together with other information, such as favoured news pages. The typical kind of accounts include banking, stockbroking and reward schemes (for example air miles). The convenience of such a service is likely to be attractive to some people, especially those with multiple accounts, who will be able to see their complete financial position at a glance. On the other hand, those who provide aggregation services and those who wish to take advantage of them need to consider the legal and security issues involved. Paragraphs 9.4 – 9.9 discuss issues for authorised firms, whilst paragraphs 9.10 – 9.14 discuss issues for consumers to consider.
- 9.3 There are two distinct ways in which aggregation services can be delivered. One involves banks, stockbrokers etc. providing aggregators with a data feed containing information about client accounts. The other involves customers providing their on-line log-on details and passwords to aggregators which then use them to access account details and make the data available to the customer. These two different models raise different questions. Although aggregating accounts via a data-feed is likely to become increasingly common

over the course of this year and next, currently it is the second approach, termed screen-scraping, which is the one mainly used within the industry, and it is this screen-scraping method of aggregation which is the focus for discussion here.

Issues for firms

- 9.4 **Authorisation issues.** The act of providing aggregation services, that is accessing a person's account or accounts and consolidating the information onto a single web-page, is not an authorisable activity. Nor does it constitute communicating a financial promotion. Therefore, any firm (authorised or not) is free to provide aggregation services. If the FSA were to develop any standards or requirements for authorised firms relating to the provision of aggregation services, non-authorised firms which offered this service, such as portals or infomediaries,¹ would be free to ignore them. The FSA can, of course, issue consumer alerts about aggregation services in general, if warnings need to be given. The FSA has already alerted firms and consumers to some of the issues they need to consider in its press release of the 15th May 2001, entitled '*New on-line account aggregation service will not be regulated, warns FSA*' (<http://www.fsa.gov.uk/pubs/press/2001/>).
- 9.5 While the act of providing aggregation services does not trigger an authorisation requirement, it is quite likely that firms which begin by providing customers simply with details of their existing accounts will want to develop the range of services offered. For example, as technology develops, an aggregator may in future be able to search the sites of on-line brokers and automatically route a buy or sell order to the broker which offers the best deal, taking into account the transaction cost and price of a security. Such a development would turn the aggregator into an arranger of deals, and arranging deals triggers an authorisation requirement. Similarly, were aggregators to provide advice about investments, authorisation would be required. Authorised firms which are not currently permitted to arrange deals or provide investment advice will need to ensure that they do not inadvertently breach their permissions by offering these services on an aggregation site.
- 9.6 **Supervisory issues.** Aggregation is a service which can be offered by any firm, authorised or not. It is also a business line that has occasioned intense reactions by financial services firms within and outside the UK. These have included concerns that the original on-line account provider will lose the customer's account, concerns about the commoditisation of financial services and the potential security threats posed by screen-scraping. The FSA is aware that there needs to be a level playing field among authorised firms, and is alive

1 These are firms which provide information about financial products and which many customers use as a first step in deciding what product to buy.

to the desirability of not developing an approach which puts authorised firms at a competitive disadvantage in relation to non-authorised firms, such as portals or infomediaries.²

- 9.7 **Legal issues.** When an aggregator scrapes the site of a firm, for example a bank, to obtain details of a customer's account, it is currently accessing both software and data on the scraped site's computer system. In the UK knowingly accessing any program or data on another person's computer without his permission is a criminal offence under the Computer Misuse Act 1990.³ To avoid committing a criminal offence, a screen scraper may obtain the scraped firm's permission to provide an aggregation service. Alternatively, the aggregator may be able to rely on permission from the bank's or broker's customer. It should be noted, however, that to avoid committing an offence under section 1 of the Act authority is required to access both a program and data. Where the customer's authority to access the data is personal to the customer and he is required not to divulge his password to anyone else, the question arises how anyone other than the operator of the computer which is being scraped can provide authorisation for a program to be accessed on its computer system.
- 9.8 The FSA's view is that authorised firms contemplating the provision of an aggregation service need to obtain expert legal advice as to whether their business model would breach the criminal law. If the view was that it would breach the law, or that it is more likely than not to constitute a breach of the law, then the FSA could not condone a firm offering an aggregation service, regardless of whether or not a prosecution might follow, and would therefore have to consider whether the firm continued to meet the threshold conditions.
- 9.9 **Security issues.** The essence of screen scraping is that consumers provide all their passwords and log-on details to the aggregator and access their consolidated account data with a single password that provides access to the aggregator's site. If this password fell into the wrong hands, it would allow some degree of access to each of the person's underlying accounts. In order to ensure that the security of a customer's on-line accounts is not compromised by the use of an aggregation service, it is vital that the aggregator's security is equally, if not more, robust than that of the most secure of the underlying individual account providers. It is also important that aggregator's security architecture takes account of likely future security strategies within the financial services industry.

Q43: Is this analysis of security issues reasonable?

2 The FSA's regard for the desirability of competition does not preclude it from expecting authorised firms to uphold high standards. The fact that high standards may be expensive need not be a competitive disadvantage. In the IT area, good security standards may be seen as a positive benefit by customers.

3 Computer Misuse Act 1990 states: 'A person is guilty of an offence if- (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that that is the case.'

Issues for consumers

- 9.10 There are four areas which have a particular consumer interest. The first and second have already been discussed. These areas are:
- a) the fact the FSA has no powers to regulate account aggregation (see paragraphs 9.4 - 9.5);
 - b) the question of whether a consumer, by using an aggregation service, diminishes the levels of security provided at his or her on-line bank or investment firm (see paragraph 9.9 above);
 - c) the question of whether the consequences of breaching an account provider's terms and conditions could result in a consumer being liable for any future errors or frauds on those accounts (see paragraph 9.11 below); and
 - d) the question of whether a consumer is aware of the data protection safeguards that operate within the European Economic Area (the EEA), and of whether he or she understands the consequences of opting out of EEA protections where aggregation services are provided from non-EEA jurisdictions (see paragraph 9.12 – 9.13 below).
- 9.11 **Legal Issues.** Screen scraping without the scraped firm's permission also raises civil law issues. The terms and conditions of many on-line service providers, including banks, explicitly specify that customers should not divulge their password, or other private security information, to third parties. An aggregator, however, asks other firms' customers to do precisely this. By signing up to an aggregation service and breaching the terms and conditions of their other on-line accounts, customers may be left liable for any future errors or fraud on those accounts, no matter how incurred.
- 9.12 **Data protection.** This raises important issues because the aggregator may have a complete picture not only of a consumer's financial position but also of his or her other interests as well, for example air miles, favourite newspapers, e-mail accounts etc. Depending on whether a consumer has opted out of EEA data protection requirements and on what data protection safeguards exist in the non-EEA country where the data is held, the extensive details collected by an aggregator could be used for cross-selling purposes that may be beneficial to the consumer or may result in the consumer possibly mis-buying highly targeted products.
- 9.13 Data protection in the UK is the responsibility of the Information Commissioner, not the FSA. Nonetheless, the FSA's responsibility for consumer protection means that it does need to consider addressing the risk that consumers mis-buy products that have been highly targeted as a result of a provider buying aggregated data. In the FSA's view it is important that those consumers who wish to use an aggregation service are given sufficient and

clear information to make an informed choice about how consumer data is being protected and the detailed consequences of agreeing to have the data being subject to non-EEA standards of protection.

- 9.14 **Questions for Consumers.** Before signing up to and using a screen scraping service, consumers would be very well advised to obtain answers to the questions on aggregation in Annex D.⁴

Possible supervisory actions

- 9.15 The FSA has explored a range of tools, or supervisory actions, that could address the risks identified in this section. The most relevant ones are: making public statements to raise awareness amongst firms and consumers of the key issues;⁵ issuing a consumer alert on the important questions consumers should consider before using an aggregation service; publishing further information on the FSA web-site; and briefing the Consumer Helpline to respond to further questions consumers may have.

Q44: Are the tools the FSA has considered using in this context the right ones? Are there any other actions the FSA should consider in relation to aggregation services?

Electronic signatures

- 9.16 Electronic signatures and other electronic trust services are important building blocks in the development of e-commerce. They address three of the obstacles which many have identified as impeding progress. These are: doubts as to the legal validity of an agreement entered into electronically;⁶ doubts as to the security of the communication; and doubts as to the identity of the counterparty.
- 9.17 Digital signatures supported by digital certificates (electronic signatures)⁷ coupled with trust services permit two or more parties communicating electronically to enter into transactions without the need for any of them to have known, met or spoken to each other. The goal is for firms and individuals to use the Internet or other similar channels to open accounts with banks or stockbrokers, to enter into contracts, make binding declarations to the tax authorities or other entities and to send payment instructions.

4 Some of these questions have already been publicised by the FSA in its press release on 15th May 2001 about account aggregation.

5 As already mentioned in paragraph 9.4, a press release on aggregation was published on the 15th May 2001.

6 Section 7 of the Electronic Communications Act 2000 removed any doubts there might have been that an electronic signature does constitute evidence that a court may take into account in determining whether or not an agreement has been entered into. It also accepts the use of 'electronic writing' generally.

7 In the rest of this section 'electronic signatures', for readability, should be taken to mean 'digital signatures supported by digital certificates'.

9.18 Four requirements are needed if e-commerce is to overcome the perceived vulnerabilities of the virtual world and command a high level of confidence. These requirements are that:

- a) communications can be transmitted securely and confidentially, so that others cannot read them, even if they are intercepted;
- b) all parties know that their counterparty is who he or she purports to be;
- c) communications cannot be altered in transmission, so that the parties have confidence that the data received is the same as that sent; and
- d) binding assent can be provided in a communication, such that the other party can act with confidence on the basis of the instruction or contract.

9.19 Providing such a set of electronic trust services – that is delivering a system which offers security, confidentiality, authenticity, integrity and non-repudiation – is currently being created around a Public Key Infrastructure (PKI).⁸ This approach to the coding or encryption of data is built around the fact that it is possible to encode data with one mathematical ‘password’ or algorithm and decode it with a different, unique but related ‘password’. In a PKI system one of these ‘passwords’ is private to the individual (frequently termed the ‘private key’). The other is made known to the counter-party (frequently termed the ‘public key’). An individual who wants to be sure that a counterparty knows a message could only have come from him, will encode some data to form a ‘signature’ with the ‘password’ known only to him (private key), and the recipient will know from whom it came, because only that individual’s publicly known ‘password’ (public key) can decode it.

9.20 However, the possession of a ‘public’ and ‘private’ key on its own provides no certainty as to the identity of any of the counter-parties. Nor does it provide any confidence that in the event of a dispute there will be any evidence linking the exchange of information to a legal entity. What provides this link between the ‘public’ key and its owner is a digital certificate issued and digitally signed by an organisation in whom people vest trust, and against whom legal action may be taken in the event that a mistake is made. PKI is the term given to the infrastructure which provides for the issuance and management of digital certificates, which give access to public keys and which provides information about certificates that have been revoked.

8 The term PKI is being used to include related technologies used in mobile e-commerce (m-commerce).

- 9.21 The process of using an electronic signature involves a number of steps. These include:
- a) the trust service provider issues a certificate;
 - b) the certificate contains the sender's public key and some attributes related to their identity (and possibly other attributes);
 - c) this certificate is provided to the relying party by some means, whether directly, for example as part of a message, or, indirectly, for example via a directory service; and
 - d) the sending party attaches a signature on the message which has been created with the private key and which is unique to that message.
- 9.22 It may be apparent that providers of trust services require high standards of systems management and controls. It is not just the IT standards for encryption which have to be robust, so must the methods of identifying individuals or firms, the process of issuing them with electronic signatures, and managing their subsequent use and cancellation. Firms providing trust services will also need to keep records for several decades in case a dispute arises and evidence is needed that a certificate was issued and that it was valid for that specific purpose on the date of use.⁹
- 9.23 There are substantial overheads in creating and operating trust services that are secure and reliable. Firms providing trust services are, in effect, guaranteeing that one or both sides of an electronic exchange of data are whom they purport to be in transactions that may be worth considerable sums of money or which may expose the counter-parties to criminal or civil sanctions. Any mistakes in the issuance or cancellation of electronic identities are likely to lead to claims for compensation.
- 9.24 Providers of trust services, therefore, carry an exposure to significant contingent liabilities. The robustness, reliability and, in part, cost of an electronic signature will tend to depend on the importance of the transaction. The use of an electronic signature to assign property rights worth millions of pounds, or to meet a legal requirement whose breach could constitute a criminal offence, is likely to require higher safeguards, than using an electronic signature to confirm that a particular risk warning was read. Those relying on an electronic signature supported by a certificate issued by a third party will need to appreciate that electronic signatures are not equal, and to know by reference to the certificate policy whether or not it is fit for the purpose in hand.

⁹ In the FSA Handbook, there are different retention periods for records of different financial products. These range from indefinite retention (e.g. for pension transfers) down to three years (e.g. for unit trusts and contract notes). The type of information that firms might be required to submit to prove the validity of the electronic signature might include: a) that the checks that were carried out when the certificate was issued were commensurate to the level of certificate issued; b) that when the certificate was validated it was indeed valid; and c) an outline of any restrictions relating to the certificate at the time it was used.

9.25 The costs of establishing robust risk management systems both as regards the issuing and maintenance of digital certificates and their acceptance for a specific purpose are likely to have an impact on the size of the market and the speed with which it grows, and the extent to which firms decide they want to use this facility.

Q45: How do you see the business to business and consumer to business markets for digital certificates developing?

9.26 Providing trust services, such as electronic signatures, is not an authorisable activity. Indeed, European law prevents EU Member States from establishing authorisation or licensing schemes for trust service providers. Any firm is, therefore, free to provide trust services. Whether or not it wants to belong to one of the accreditation schemes available or being set up, is a matter for its commercial judgement. The FSA has no direct interest in laying down technical standards with which trust service providers should comply. However, there are a number of risks to the FSA's statutory objectives which could arise from the use or misuse of electronic signatures and the FSA cannot be indifferent to how these risks are mitigated.

9.27 These risks arise in four areas:

- a) money laundering and other types of financial crime;
- b) the provision of trust services, including the issuance of certificates supporting electronic signatures, by authorised firms;
- c) the acceptance by authorised firms of electronic signatures issued by other firms; and
- d) the use of electronic signatures by individuals and firms in their ordinary day to day activities.

Money laundering

9.28 The use of digital certificates as a means of providing evidence of a person's identity for the purposes of conducting business on-line, raises a number of concerns regarding UK money laundering requirements. The E-Commerce Theme and the Money Laundering Theme have co-ordinated their efforts to identify the legislative, regulatory and prudential risks associated with the use of digital certificates and electronic signatures and to outline a possible way forward.¹⁰

9.29 Most regulated firms are already required to comply with the money laundering regulations 1993 (the Regulations). Once the Financial Services

¹⁰ In this paper, wider data protection issues are not discussed. The Office of the Information Commissioner has lead responsibility in this area.

and Markets Act 2000 (FiSMA) comes into operation, they will also have to comply with money laundering rules (the Rules) set out in the FSA's Money Laundering Sourcebook.

- 9.30 Both the Regulations and the Rules set out firms' duties in relation to the prevention and detection of money laundering. These have direct implications for the use of a certificate issued by a third party provider of trust services, particularly in relation to customer identity verification and record keeping. A 'relevant firm'¹¹ which breaches the Regulations or Rules may be subject to criminal or regulatory enforcement action by the FSA.
- 9.31 Because the Regulations and Rules impose largely general duties on firms, the Joint Money Laundering Steering Group's (JMLSG) Guidance Notes play a key role in setting out detailed policies and procedures for 'relevant firms' to follow in order to meet their legal and regulatory obligations. Where the Regulations are concerned, a court may take compliance with the Guidance Notes into account in deciding whether a firm has properly identified a customer. The FSA's Enforcement manual explicitly refers to the Guidance Notes, stating that when considering whether to take disciplinary action for a breach of the Rules, the FSA will have regard to whether a firm has followed relevant provisions in the Guidance Notes.
- 9.32 In practice, therefore, the JMLSG Guidance Notes will heavily influence the extent to which an electronic signature supported by a certificate which is issued by a third party can be used for identity verification purposes. The February 2001 edition of the Guidance Notes, whilst setting out what kinds of electronic checks may be performed on a new customer, does not address the acceptability of digital certificates. This is not a serious omission at present, since large scale PKI infrastructures for financial services are in the process of being established. However, the use of electronic signatures does raise important questions which need to be addressed and the FSA is interested in receiving views in this area.

Q46: Should it be possible for an electronic signature supported by a certificate issued by a third party, which has complied with the non-face to face requirements set out in the JMSLG Guidance Notes, to be relied on by a relevant firm as evidence of identity, sufficient to enter into a relationship with the customer? Does this obviate the need for any further checks to be performed before an account is opened?

11 A 'relevant firm' is defined in the FSA's Money Laundering Sourcebook. This Sourcebook contains the FSA's money laundering rules.

Q47: Alternatively, might such a signature require only a reduced number of checks to be performed, for example a single check on the address for fraud purposes, or one check on an address and another on identity?

Q48: If an authorised firm can rely on an electronic signature issued by a trust service provider in the UK for the purpose of entering in to a relationship with a customer, should an authorised firm also be able to rely on such a signature where the certificate is issued by a trust service provider outside the UK? If so, should any additional checks be required, and, if so, in what circumstances?

9.33 The issuer of a digital certificate of identity will need to validate that person's identity. The question arises as to which identity related attributes should actually be in, or held to support, the certificate. Authorised firms require a range of information on opening an account. Some of it can simply be attested to by the applicant (e.g. security-related information, such as the mother's maiden name). Some information will need to be associated with the certificate in order to allow firms to be satisfied of the identity of the subject. These might include name, full postal address and date of birth.

Q49: What identity related attributes do you believe should be held in or to support the certificate?

9.34 Before an electronic signature issued by a third party could be used to allow customers to enter into a financial relationship with a firm, it is not enough for the JMLSG to have decided how many, if any, additional checks need to be performed and what information should be held in the support of the certificate. There are a number of other risks that need to be identified and then managed, if reliance were to be placed on an electronic signature. These risks include:

- a) firms fail to establish identity due to a failure in the quantity or quality of (registration) checks they perform;
- b) a certificate issued by a third party is accepted by an authorised firm for a purpose that goes beyond its scope;
- c) firms issuing certificates fail to have effective systems in place to ensure that there have been no changes which would invalidate the certificate of identity for a particular purpose (for example, in respect of account opening, a change of address);
- d) a certificate is not valid at the time of use either through revocation or compromise of the certification authority's systems and controls;
- e) the issuer's records may not be properly kept, with the result that law enforcement agencies would find it difficult to establish later what

evidence had been relied on when a fraudulent signature was provided (see footnote 9 on record keeping requirements);

- f) the trust service provider's system may be unavailable, causing disruption to the process of validating the certificate; and
- g) the issuer of the digital certificate is a criminal enterprise.

Q50: Are there any other material risks arising from the use of electronic signatures that are related to money laundering or to the need to reduce financial crime?

Q51: As regards record keeping, what requirements and arrangements should there be to ensure that years or several decades later it can be shown that a certificate had been properly established, and that it had been checked and found valid at the time of use? What services supporting such verification, if any, need to exist before the acceptance of electronic signatures is allowed?

9.35 In the FSA's view if a digital certificate is to be used to allow customers to enter into a financial relationship with a firm, ensuring its ongoing integrity is as important as performing the required identification checks. For example, a digital certificate that had been properly issued nine months previously, would be useless if the issuer did not also have adequate systems in place to ensure that it had not subsequently been compromised. Furthermore, if attributes contained within the certificate of identity were being relied upon, firms would have to be confident as to its scope and that the trust service provider was accurately updating and retaining its records.

Q52: Is the on-going integrity of a digital certificate as important as the identity checks when the certificate is issued?

9.36 The way forward. In line with the need to have regard to the desirability of innovation and competition, the FSA considers it important that an effective regime be established enabling digital certificates issued by third parties to be used by customers wanting to enter into financial relationships with authorised firms. This should reduce costs of account opening for firms and help make financial markets more competitive.¹²

9.37 However, one of the FSA's statutory objectives is to reduce financial crime, and firms for their part, though likely to view positively proposals that reduce costs, will not want to risk criminal prosecution or regulatory discipline for breach of the Rules. Furthermore, section 150(1) of the FiSMA permits a private person who suffers loss as a result of a contravention of an FSA rule by an authorised firm to take legal action against that firm. A loss resulting from a breach of the Rules would be actionable under this section.

12 The Cruickshank Report, published in March 2000, recommended that the use of new technologies, such as digital certificates for identity verification, should be examined as a means of enhancing competition.

- 9.38 Before electronic signatures issued by third parties can be used for entering into a financial relationship, standards, controls and procedures will need to be in place to ensure that the following objectives are met. These are:
- a) confidence in registration practices (including whether satisfactory identity checks have been carried out);
 - b) confidence in the certificate policy (including clarity about the purposes for which the issuer is warranting the certificate of identity);
 - c) confidence as to the validity of the certificate of identity at the time of use; and
 - d) confidence in the practices and procedures of the issuer of the certificate (the certifying authority).

Q53: Are these objectives reasonable ones? Are there any other key objectives that need to be met?

- 9.39 There are a number of bodies involved in drawing up standards for the provision of trust services. These include: the European Electronic Signature Standardisation Initiative (EESSI), supported by Centre Européen de Normalisation (CEN) and the European Telecommunications Standards Initiative (ETSI) which are developing standards to support the EU's Electronic Signatures Directive; Global Trust Authority (GTA), an international consortium that will provide trust services in the corporate market; Identrus, an international consortium that will provide trust services within the corporate market; and t'Scheme, the voluntary accreditation scheme for electronic trust services being established in the UK.
- 9.40 After consulting with groups such as these, the FSA will wish to discuss with the Joint Money Laundering Steering Group (JMLSG) the question of the standards which trust service providers must meet before their certificates of identity can be relied upon for the purpose of financial relationships being entered into.
- 9.41 However, the JMLSG will also need to determine how authorised firms can be confident that issuers of electronic signatures do meet the necessary standards in practice. Where an activity, such as the provision of trust services, is not subject to compulsory regulation, necessary confidence may be achieved by trust service providers being audited against the relevant standards by suitably experienced auditors. This would mean that authorised firms would need to take steps to be sure to know whether or not a trust service provider had been regularly audited against an appropriate technical standard and to know the results of that audit. Alternatively, where the trust service provider is a member of an organisation that itself requires regular audits against such a

standard, the firm would need to check that it was still a fully accredited member of such a scheme and met UK money laundering requirements.

Q54: Are there any other non-compulsory ways in which authorised firms could use electronic signatures and certificates for the purpose of entering into financial relationships in the confidence that they were complying with the money laundering regulations 1993 and FSA's money laundering rules?

9.42 It should be stressed that authorised firms wishing to accept electronic signatures issued by third parties may need to review their internal procedures to ensure that signatures which do not meet the necessary standard are not accepted.

Q55: Do you support the approach laid out above for ensuring that proper controls and procedures are put in place so that digital certificates of identity can be relied upon for the purpose of entering into financial relationships? Could the approach be improved, and if so how?

Q56: Does this approach take sufficient account of the differences between the use of electronic signatures in the business to business and consumer to business sectors?

Q57: In order to ensure that authorised firms have time to develop the processes and controls suggested above, what would be a reasonable time-scale for drawing up guidance in this area?

Q58: How do authorised firms propose to address the risk that a customer does turn out to have been laundering money using an account opened on-line, despite operating whatever controls are recommended?

Authorised firms as providers of trust services

9.43 A number of banks have already announced that they will be providers of electronic trust services, and will therefore issue digital certificates which warrant, for a defined period of time, that a particular person, in an individual or corporate capacity, is who he purports to be in respect of that transaction. Although providing a trust service is not a regulated activity, an authorised firm that has issued thousands, or in time millions, of signatures is exposing itself and ultimately depositors, investors or policy holders to considerable risk, in the event that it failed to control these risks properly.

9.44 The FSA is interested in how authorised firms will identify and manage risks associated with the provision of trust services, especially if such risks might crystallise into actual liabilities. Where firms choose to outsource their

provision of trust services to a third party, firms will need to make sure that they comply with the requirements underlying FSA's guidance on outsourcing. The kinds of areas which issuers of certificates supporting electronic signatures may need to address include:

- a) standards of security;
- b) operating procedures for the issuance and management of certificates;
- c) processes for amending, recalling and cancelling digital certificates;
- d) record keeping and audit trail for long term contracts;
- e) warranty liability monitoring;
- f) disaster recovery and business continuity;
- g) adequacy of audit and accreditation;
- h) crisis management procedures;
- i) insurance against successful claims; and
- j) setting aside capital for any claims that might crystallise.

Q59: Are there other key areas issuers should address?

9.45 The FSA will take a keen interest in how effective authorised firms prove to be in identifying and controlling risks such as these. The tools which the FSA could deploy include: themed visits so as to benchmark good practice; dissemination of good practice; firm monitoring; and review by experienced external IT auditors in appropriate cases. The FSA might also have regard to membership of an industry or accreditation group, which itself had good standards and monitored its members' compliance with them, and where the FSA had access to the results of such monitoring. Where it appears that a failure by a firm to control the risks related to providing trust services might put depositors, investors or policy holders funds at risk, the FSA will take appropriate action.

Q60: Are these appropriate tools for the FSA to use? What other tools might it consider adopting?

Q61: What kinds of information, if any, would firms wish the FSA to provide to any accreditation agency, were there to be information sharing arrangements which aimed to reduce regulatory duplication on the part either of the accrediting agency or the FSA?

Accepting digital certificates issued by other firms

- 9.46 The use of electronic signatures supported by certificates issued by third parties for the purpose of entering into a financial relationship has already been extensively discussed. However, there are other uses to which electronic signatures may be put. The FSA Handbook provides guidance in GEN 2.2.15G¹³ that:
- ‘electronic media may be used to make communications which are required by a provision of the Handbook to be ‘in writing’, unless a contrary intention appears, or the use of electronic media would contravene some other requirement such as the requirement to treat customers fairly under Principle 6.’¹⁴*
- 9.47 This guidance will be relevant in all areas where the FSA currently requires authorised firms to obtain a signature.
- 9.48 Where firms are relying on an electronic signature as being equivalent to a wet (hand-written) signature, they will need to ensure that the certificate supporting the electronic signature they accept, has been issued to a standard that enables them to place reliance on it and that it is still valid and has not been amended, suspended or revoked. Firms will therefore be prudent to have in place systems that check the certificate’s validity with the issuer as regards the time, identity, and purpose for which it is presented. Firms will also want to ensure that a record is kept that such a check was made as well as the result of that check.
- 9.49 There are a number of areas where the FSA does not impose a requirement for a signature. In these circumstances it is up to firm to decide how secure a level of affirmation is appropriate. Nonetheless, there may be circumstances where firms might be prudent to consider whether or not a wet signature is required, for example to reduce the risk of fraud. Such circumstances include:
- a) issuing a debit card for an account opened remotely, where a firm does not have a record of a customer’s wet signature; and
 - b) issuing a cheque book for an on-line current account, where the firm does not have a record of the authorised signature.
- 9.50 Electronic signatures are merely one way in which a client of a firm may provide an electronic affirmation. Forms of electronic affirmation that fall short of an electronic signature include clicking on an ‘OK’ or ‘I accept’ button. It may be observed that these forms of electronic affirmation will on their own not provide any confidence that the entity clicking on an ‘OK’ button is who he or she purports to be. Lower levels of confidence may be

13 See Policy Statement : General Provisions (April 2001).

14 Principle 6 states ‘a Firm must pay due regard to the interest of its customers and treat them fairly’.

entirely appropriate where a firm is using a form of registration to obtain marketing information.

- 9.51 The FSA Conduct of Business Sourcebook provides further guidance in respect of investment firms which covers electronic communication more generally. COB 1.8.2G states that:

‘For any electronic communication with a customer, a firm should:

- (1) have in place appropriate arrangements, including contingency plans, to ensure the secure transmission and receipt of the communication. It should also be able to verify the authenticity and integrity of the communication. The arrangements should be proportionate and take into account the different levels of risk in a firm’s business;*
- (2) be able to demonstrate that the customer wishes to communicate using this form of media; and*
- (3) if entering into an agreement, make it clear to the customer that a contractual relationship is created that has legal consequences.’*

Using electronic signatures in the course of business

- 9.52 Authorised firms may wish to use and accept electronic signatures in the course of their daily business, for example, with their suppliers and partners. This is not an area of major regulatory interest. Nonetheless, in such circumstances staff who are provided with a digital signature by the firm will have the power to commit the firm to contracts. A firm will wish to have adequate high level controls in place to ensure that it can monitor both the type and number of contracts to which it is being committed and the amount to which it can be committed by particular employees.

Q62: Have firms considered how current operational discretionary powers possessed by authorised signatories will be mapped into the digital world?

Q63: How are firms planning to maintain an audit trail of digital transactions carried out by staff or computers?

The use of electronic signatures by consumers

- 9.53 Responsibility for electronic signatures lies with the DTI, which piloted the Electronic Communications Act 2000 onto the statute book. It is the DTI which is sponsoring t’Scheme, the industry based accreditation scheme, on whose board the Cabinet Office sits. While there is a considerable amount of work that will need to be undertaken to inform consumers about how

electronic signatures work and how to keep them secure, it is arguable that the FSA has a minor role in this area, since a non-authorized firm may issue an electronic signature and a consumer use it in a transaction with a non-authorized firm.

- 9.54 However, the Financial Services Ombudsman has indicated that he will consider claims related to digital certificates in so far as they are issued, accepted or used by authorized firms in relation to authorized business and that the complainant is eligible under the terms of the ombudsman scheme.
- 9.55 The FSA will need to consider whether it should be good practice for firms to set out their dispute resolution mechanism in this area for their customers. The FSA acknowledges that these may differ for the business to business and business to consumer markets.

Q64: What should issuing firms' responsibilities be in this area? What else could be done, and by whom, to aid public understanding?

Top-level domains (TLD)

- 9.56 In the last quarter of 2000, Internet Corporation for Assigned Names and Numbers (ICANN)¹⁵ invited applications for new generic Top Level Domain names.¹⁶ This had been in response to the expansion of web-site creation putting pressure on the existing addressing system and giving more weight to the view that the current addressing system was no longer sufficient to mirror the diversity of web-sites available. Applicants could either propose a 'sponsored' TLD (where ICANN delegated the release of the domain name to a sponsoring authority) or an 'unsponsored' TLD (where policy formulation with respect to the release of the TLD remains with ICANN).
- 9.57 During the application process for TLDs, there was some limited consideration by financial services supervisors in various jurisdictions as to whether the sponsorship of a 'financial' TLD was something which the supervisory community wished to pursue. The paragraphs which follow, set out some of the benefits and costs which were considered. It was decided at that time by those regulatory authorities that sponsorship of a financial TLD was not something they wished to pursue.¹⁷
- 9.58 At present it is not clear when ICANN will re-open the application process for TLDs, but it is likely they will do so at some future point in time. In light of

15 The global regulator of top-level domain names – further information may be found at <http://www.icann.org>

16 Top-level domain names are the final section of Internet addresses. There are two main types, country code top-level domain names, e.g. '.uk', '.nz', '.fr', or generic top-level domain names, e.g. '.org', '.com'. This section focuses on generic top-level domain names, which are referred to in this section of the paper as TLDs.

17 It should be noted that the Association des Banques Monagasque did make a formal application to ICANN for the sponsorship of '.fin' but this proposal was subsequently rejected by ICANN.

this, the FSA has undertaken analysis as to whether a financial TLD (from this point forward referred to as ‘.fin’) would be a regulatory tool which the FSA could use in the achievement of its statutory objectives. Set out below is a short discussion of the benefits and costs of a regulator sponsored TLD. In Annex E there is more detail on the analysis undertaken by the FSA in its assessment of ‘.fin’ as a tool for mitigating risks to the FSA’s objectives.

- 9.59 **Benefits.** At present a financial services firm’s web-site and web-site address may not clearly disclose whether it is authorised, and if it is, the name and contact details of the relevant regulator. The introduction of a TLD, sponsored by regulators, could give consumers a reliable ‘short cut’, that would disclose regulatory status, and if combined with a country code, the jurisdiction in which it is authorised. There are other methods of helping consumers assess whether they are dealing with authorised firms, hyperlinks is one example (see paragraph 8.29). The use of .fin should be considered in relation to these other methods.
- 9.60 Another potential benefit is in the area of enforcement. If the regulator controls the release and removal of .fin, those firms holding themselves out to offer regulated financial services via the Internet without the correct authorisation will be easier to identify both for consumers and for those in regulatory and/or law enforcement agencies charged with policing the perimeter. There could be considerable advantages in establishing a system of web addresses that made it easier to conduct surveillance of the Internet, and more difficult for spoof sites or look-alike sites to be set up, or which reduced the length of time in which scams claiming to be authorised firms could defraud the public.
- 9.61 **Costs and Risks.** For the benefits of ‘.fin’ to be fully realised, however, it is important that all users have a full understanding of what it does and, more importantly, does not mean. For example, whilst a firm’s authorisation by a regulator may indicate that certain minimum standards have been met by that firm and may also indicate access to compensation schemes, authorised firms do not share the same risk profile. Furthermore, the fact of authorisation one day does not necessarily mean that a firm is not facing enforcement action or commercial pressure which could result in it ceasing to be authorised. In addition, authorisation to undertake one regulated activity, for example deposit-taking may not necessarily mean a firm is permitted to undertake another regulated activity, for example providing investment advice. Finally, not all financial services are regulated (for example bureaux de change in the UK) and different jurisdictions vary over what they subject to regulation (see chapter 4 on International context). In order for there to be confidence in ‘.fin’, those responsible for its administration would have to ensure that users had full and realistic expectations of what this TLD name signified.

- 9.62 Many firms have spent considerable sums to ensure brand name recognition of their URL.¹⁸ Changing a URL and promoting the new address would cost money. Internationally active firms would also have to decide which URL to use when selling multiple products requiring multiple authorisation in multiple jurisdictions all from one site – arguably, one of the benefits of using the Internet to sell financial products.
- 9.63 Finally, there are issues which arise from the practical aspects of using a regulator sponsored TLD and which would need to be considered, not least from a cost/benefit point of view. They include:
- a) **Responsibility for the administration of the release and withdrawal of the TLDs.** The question of responsibility is of particular importance in the case of the withdrawal or revocation of authorisation. In this situation, it would be essential that a firm could not use a .fin address the moment it had ceased to be authorised. Other issues that would need to be resolved include: how and by whom a TLD was controlled and monitored, and what co-ordinating mechanisms regulators would need to establish. For example, would each individual regulator control the release of the TLD for its jurisdiction or would a central body do it? The issue of responsibility would also need to be considered in relation to those jurisdictions where the regulation of financial services is divided between different agencies;
 - b) **Transitional Confusion.** Would the potential cost to firms, which have already invested substantial amounts in domain name recognition, and the initial confusion that would be caused amongst their customers, be likely to be justified by the potential benefits? (For example, whilst it should be relatively straightforward to link bank.com through to bank.fin, if customers had been informed that unless a firm had .fin at the end of its domain name, they may erroneously regard a firm transitioning from .com to .fin as not authorised); and
 - c) **EU Arrangements.** If it were required that there should be a country suffix with a financial TLD, agreement would be needed within the EU about the use of a .fin country code. For example, would a firm using its passport to provide financial services to another Member State have to use the country specific suffix in each market it was targeting, or would it be permitted, but not required, to do so, or would it not be allowed to do so?
- 9.64 In light of these considerations and in light of the toolkit analysis detailed in Annex E, the initial conclusion is that sponsorship of ‘.fin’ is not an initiative the FSA wishes to pursue at present. However, this decision does not preclude

18 Uniform Resource Locator, the global address of documents and other resources on the World Wide Web.

the FSA from being involved in further discussion with other regulators on this issue nor from reconsidering its position should current circumstances change.

Q65: Is the analysis of the advantages and disadvantages correct?

Q66: Is the FSA's view of whether it wishes to sponsor '.fin' the correct one?

Are there any other considerations that are not mentioned in this section or in Annex E that the FSA should take into account in its analysis of the use of TLDs?

FSA's existing work and initiatives

- A.1 The FSA and its constituent organisations have been at the forefront of attempts by regulators internationally to identify risks arising from e-commerce and respond constructively to them. The specific regulatory issues prompted by e-commerce varies according to the sectors. Particularly within the banking sector, policy has been developed within an international framework, and these initiatives are discussed in Annex B. This annex (Annex A) provides a brief description of the regulatory work done over the last four years in the areas of authorisation, banking supervision, investment business, markets and exchanges, authorisation enquiries, enforcement, consumer relations, general insurance and listing.
- A.2 **Authorisation of firms.** Firms which operate wholly or to a material extent via the Internet are highly vulnerable to the technology on which their business is based. A series of IT failures, or a single serious one, could do significant commercial damage to firm's reputation and customer base. It might threaten the firm's existence. The FSA and its constituent organisations, when authorising a firm, have to be satisfied that it meets the relevant minimum threshold conditions for authorisation. These include a requirement that the firm has adequate systems and controls – including IT systems and controls – in relation to the nature and scale of its business.
- A.3 For the last two years, the FSA has required firms applying for authorisation and intending to provide services via the Internet or similar electronic means to complete a detailed e-commerce business and systems questionnaire, which has been developed by the FSA. The questionnaire focuses firms on all aspects of IT systems and controls and the way in which their systems are managed. The areas covered by the questionnaire include: project management; systems security; IT recovery procedures; system availability; and change control procedures (see also paragraph 6.26).
- A.4 **Authorisation enquiries.** The Internet makes it easier for firms which have not been traditionally involved in the provision of financial services to enter that

market. This has led the FSA to receive a number of enquiries from non-authorized firms concerning the kinds of activities which can be undertaken without triggering an authorisation requirement. The main focus of attention has been a new business sector – the infomediaries. These are firms which provide information about financial products and which many customers use as a first step in deciding what product to buy. Two questions have often arisen. The first is whether infomediaries can take advantage of the exemption in the Financial Services Act 1986 which permits periodical publications to provide investment advice so long as such advice is not the principal purpose of the publication. The new Financial Services and Markets Act 2000 (FiSMA) provides helpful clarification by specifying that the principal purpose exemption covers advice not just in writing but also in other legible forms, and also when provided by way of a service comprising regularly updated news or information.

- A.5 The second question concerns the arranging of deals. A number of Internet Service Providers, portal sites and infomediaries have been in touch with the FSA to determine what their position is under UK legislation. The Internet places portal sites and especially infomediaries in a very attractive position to organise for their customers special deals with investment firms. Introducing a member of the public to an authorised firm may often constitute arranging deals, an activity which triggers an authorisation requirement. The FSA has spent considerable time providing firms with guidance as to what the law in this rather difficult area does and does not permit infomediaries to do without authorisation.
- A.6 **Banking.** Supervisors have reviewed firms' e-commerce services on a risk basis in a number of ways, including meetings with management and IT staff, the use of the systems questionnaire (see paragraph A.3 above), on-site visits by the FSA's IT risk review specialists, and reports on IT systems and controls commissioned from external audit firms. Important issues addressed by supervisors in their recent work include:
- a) the place of Internet mediated banking services within firms' overall IT strategy and IT organisation;
 - b) the project management framework for new Internet service initiatives;
 - c) the security arrangements for the service (architecture and administration);
 - d) business continuity and disaster recovery arrangements;
 - e) capacity planning ahead of launch;
 - f) the methodology for testing ahead of launch and for controlling subsequent changes to its e-commerce offering;

- g) the review and coverage of IT and e-commerce services by a firm's audit and compliance departments; and
 - h) the controls over outsourced IT functions supporting e-commerce services.
- A.7 **Peer group reviews.** To complement the supervision of firms on an individual basis, the FSA has carried out two peer group reviews.¹ The results of these reviews were fed back to the firms concerned and the findings disseminated to staff in the FSA. These reviews also informed FSA public speeches on e-commerce and articles on e-commerce controls.
- A.8 **Investment business.** The area in which the Internet has had the greatest market impact in the investment business sector, is e-broking. Firms are now allowing their customers to buy and sell shares on an execution only basis via the Internet. The large banks as well as traditional brokers have been developing Internet operations, and there is also a number of brokers which provide Internet-only services.
- A.9 On-line trading now represents about 29 per cent of all execution only transactions. Whilst there has been growth in the advisory and discretionary sectors, growth rates of execution only trades have increased considerably more.
- A.10 The Internet has not just seen a shift in the way in which customers interact with markets and a fall in the cost of trading. It has also drawn new people into the equity markets. One indicator of this is the fall in the size of the average on-line trade. This has reduced from £13,752 in the first quarter of 1998 to £3,400 in the second quarter of 2000.
- A.11 The other area of significant e-commerce activity has been the growth of investment supermarkets. Firms are now marketing a range of provider's funds via the Internet. A number of product providers are also using the Internet to market and sell their own packaged funds, such as unit trust and Open Ended Investment Collective Schemes (OEICS).
- A.12 **Regulatory responses in the investment business sector.** Investment services regulators have been providing formal guidance on the Internet since 1997.² The guidance varies between the stockbroking, fund management and IFA and life office sectors. The main focus within the IFA and life office sector has been to supervise compliance of firms' web-sites with the advertising and

1 The first review assessed strategy, group risk assessment and security practices relating to e-commerce in a group of major firms. It covered the areas discussed in paragraph A.6 in considerable detail and benchmarked practices between firms. The second review focused on business to business e-commerce, in particular the risks and controls in on-line wholesale trading. The areas covered included: the use of control processes, such as new product approval processes; the effects on credit risk systems and processes; the connections between e-commerce applications and other internal processing and risk systems; and, the use of Internet based developments to improve back office processes.

2 This includes Guidance Releases from PIA, IMRO, and SFA. Their contents are not summarised here, since it has been developed and finds current expression in the Conduct of Business Sourcebook which will come into operation when the new legislation comes into force later this year.

marketing requirements, to ensure, in particular, that the required information and key features material are provided in suitable ways and that the sites are clear, fair and not misleading. Fund supermarkets have highlighted issues, such as how best to disclose detailed information on the range of products available, how to distinguish between advice and information, and what type of firm could offer a supermarket service.

- A.13 In the area of stockbroking a considerable amount of regulatory guidance has been provided. This includes:
- a) advising firms to discuss with the regulator their plans prior to starting a new service over the Internet;
 - b) advising firms to undertake appropriate monitoring of any bulletin boards they operate;
 - c) advising firms that have hyper-links to sites which are not subject to UK regulation that they need to provide a warning that the customer is leaving the firm's site with its associated UK regulatory protections;
 - d) clarification on the circumstances in which repeat acceptance of risk warnings is required; and
 - e) clarification on the circumstances in which firms must store records of market data carried on their web-site.
- A.14 **Markets and exchanges.** Electronic order routing systems to electronic market places pre-date the use of the Internet by financial service firms. Because exchanges and clearing houses occupy a critical position in the financial infrastructure, the FSA and its predecessor organisations have addressed on an individual basis relevant IT security, capacity and resilience issues for a number of years. The tools used are individual supervision, scrutiny by the FSA's IT risk review specialists and, where appropriate, audit of a specific issue by external consultants. The Recognised Investment Exchange (RIE) and the Recognised Clearing House (RCH) Specialist Sourcebook, covering regulated exchanges and clearing houses, has recently been updated to include guidance on IT systems and controls (see extract in Box 2 on page 36).
- A.15 **General Insurance.** The statutory focus of the FSA's regulation of general insurance is prudential, aiming to protect policyholders by ensuring that businesses are soundly run and financially secure.³
- A.16 The distinctive features of e-commerce on this aspect of regulation are more limited than for conduct of business regulated industry sectors. However, e-commerce is a factor taken into account by supervisors in examining the business strategy of firms and the risks they pose. E-commerce is profoundly

³ Regulatory issues to do with selling general insurance products are the province of General Insurance Standards Council.

affecting the way in which insurance is sold and there will be winners and losers among firms. Supervisors seek to identify signs of stress in those firms coming under financial pressure whether by competitive pressure on margins, loss of market share or costly investment in new technologies.

- A.17 Another issue which is assuming importance is ensuring that firms who engage in cross-border trading are properly authorised to do so. The rules which govern this issue are derived from European Directives.
- A.18 **United Kingdom Listing Authority (UKLA).** The FSA is the UK's competent authority for listing. It makes rules (the 'Listing Rules') governing the admission of securities to listing, the continuing obligations of issuers, the enforcement of those obligations and the suspension and cancellation of listings.
- A.19 The FSA has responded to the challenge of e-commerce as regards its listing responsibilities. In January 2000 it introduced a new chapter to the Listing Rules. The new provisions sought to allow innovative, high growth companies to list, even where they have not had the three year trading record usually required. Approximately 30 companies were admitted through this concessionary route to listing in the first year of operation of the new rules.
- A.20 **Enforcement.** The FSA's enforcement function embraces surveillance to identify potential wrongdoing; investigation of attempts to abuse regulated markets, or to promote or provide people in the UK with regulated financial services in breach of UK requirements; and enforcement action, in appropriate circumstances; and, where possible, restitution for consumers.
- A.21 The FSA uses all sources of intelligence to identify activities that may be in breach of UK requirements, whether these take place on-line or off-line. In addition, and as a departure from a strictly technologically neutral approach, the FSA conducts surveillance sweeps of the Internet.⁴ Analysis of the two largest sweeps undertaken showed that 94 web-sites were identified as requiring review. On analysis, almost 40 per cent were not undertaking activities in breach of UK requirements. Around 30 per cent of sites were not in breach of FSA requirements but aroused suspicions and were referred to other agencies, either abroad or in the UK. Of the remainder, 15 per cent are still under active consideration, and action has been taken in the other 15 per cent.
- A.22 Effective surveillance and enforcement requires active co-operation and training. The FSA has established links with a number of organisations, including: the Metropolitan and Merseyside police's specialist computer crime units; the National Criminal Intelligence System; Internet service providers;

⁴ The FSA does not conduct general surveillance of other communications channels, e.g. the post or telephone, to see whether UK requirements are being breached.

industry e-crime working groups; and the FBI. The FSA has also participated in international enforcement training events in the UK and USA.

- A.23 **Consumer relations.** The Internet presents opportunities and risks to consumers. Many of these are not new in themselves, but they may require new responses. The FSA has focused on three areas in particular. These are: the FSA's web-site; the Central Register of authorised firms; and the development of comparative indicators on packaged products.
- A.24 The FSA's web-site (<http://www.fsa.gov.uk>) has a consumer help section with specific pages on e-commerce. These include pages covering tips on on-line shopping, investing on the Internet, and the risks of believing everything that appears on bulletin boards and chat rooms.
- A.25 The FSA's web-site also has a hyperlink to the FSA's Central Register. This contains details of all UK authorised firms and may be accessed by telephone or directly on-line at: <http://www.thecentralregister.co.uk> (registration is necessary). Perhaps the single most important step consumers can take prior to parting with their cash is to check that a firm is authorised, since access to the ombudsman scheme and the compensation safety net is limited to customers of authorised firms.

International fora

- B.1 The following paragraphs summarise the scope of current initiatives in the international arena concerning e-commerce.

The European Union

- B.2 The European Union has undertaken a significant amount of work in order to deepen the single market and respond to the development of e-commerce delivery channels. Under existing single market legislation firms authorised to do business in one Member State have the right to establish themselves in any other part of the European Economic Area (the EEA) and to do so under the authorisation and prudential oversight of their home state, that is the country where the firm has its head office and registered office. The home state's compensation scheme may also provide compensation in the event that a credit institution or investment firm goes into default.
- B.3 EEA firms also have the right to provide services to other Member States on a services basis, that is without a permanent establishment in the state where the recipient of the service is based. However, whether they provide services from a branch or remotely on a services basis, firms must comply with the applicable conduct of business requirements that operate in the Member State where the recipient of a service is based.¹ The content of these rules varies considerably from one country to another and from one service to another. For example, in the banking sector there are very limited regulatory requirements in the UK relating to disclosure compared to those that operate in the investment business arena. In the insurance sector, conduct of business requirements vary considerably from one Member State to another.

1 As described in chapter 4, the requirements with which an EEA firm operating cross-border on a services basis will have to comply will depend on whether a promotion is being communicated to people in another Member State or whether the service itself is being provided in that other Member State.

- B.4 The effect of existing single market legislation is that firms wanting to provide financial services across the EEA will need to ensure that their web-site complies with the different requirements in operation in each of the different Member States.
- B.5 The European Union recently approved the Electronic Commerce Directive (ECD), which has to be implemented by Member States by 16 January 2002. This Directive applies to all services provided by Internet and e-mail, not just financial services. It will have a significant impact on which Member State's pre-contractual requirements apply in the provision of financial services.
- B.6 The main differences between the current situation and the position under the ECD will be:
- a) each Member State will have to ensure that financial services provided by firms comply with those requirements which fall within the Directive's 'co-ordinated field';² and
 - b) Member States where the recipient of a service is based will no longer be able to impose their requirements on services provided from another Member State, in so far as these requirements restrict the freedom to provide a service and fall within the Directive's 'co-ordinated field'. The result is that firms will be able to provide financial services across the EEA from a single web-site that complies with the requirements of the Member State from where the service is provided – the 'country of origin' approach.
- B.7 The Directive has a very broad sweep and it will not always be immediately apparent which requirements restrict the freedom to provide a service and fall within the ECD's 'co-ordinated field', and which ones fall outside it. Requirements which fail to meet these two conditions can continue to be imposed by the Member State where the recipient of a service is based.
- B.8 There are other significant derogations³ from the country of origin approach. These include contractual obligations concerning consumer contracts, direct insurance services, the permissibility of unsolicited e-mail, e-money institutions, and advertising requirements imposed on Undertakings for Collective Investment in Transferable Securities (UCITS) product providers. (Passported intermediaries, rather than product providers, can use the ECD to sell UCITS on the basis of their country of origin requirements.) In all these situations the country where the recipient of a service is based will continue to be able to apply their own requirements.

2 The full definition of the 'co-ordinated field' is given in Article 2(h) of the Electronic Commerce Directive (ECD). It covers general and specific requirements, including those relating to the taking up and pursuit of an information society service.

3 i.e. exemptions from the requirements.

- B.9 There is also a derogation permitting Member States to impose their own requirements, but only on a case by case basis and where a number of tests have been met.⁴ The Commission is concerned to ensure that while the Community adapts to the country of origin approach standards of consumer protection are not compromised. The Commission is consulting Member States on how this derogation might best be used until greater convergence in the standards of consumer protection has been achieved across the EEA.
- B.10 One area in which greater convergence is currently being negotiated concerns the marketing requirements imposed on firms. The draft Distance Marketing Directive (DMD) proposes a number of areas in which a common set of information requirements would apply across the Community in the banking, investment and insurance sectors. The DMD applies to all non-face-to-face marketing, not just the supply of services over the Internet. Some of these information requirements would be subject to maximum harmonisation, with the result that Member States would not be allowed to add their own requirements. Others would be harmonised but would allow scope for Member States to impose additional information requirements in specified areas. The result of the Directive, when it is agreed and comes into force, should be to develop further Europe's single market in financial services and reduce the cost on firms of having to prepare marketing material to the different specifications of each Member State.
- B.11 This very brief overview necessarily skates over some very complex issues. The FSA is devoting considerable resources to preparing for the further enhancement of the single market, for example through the revision of the Investment Services Directive, further harmonisation of conduct of business requirements and the work plans proposed in the Commission's Communication on e-commerce and financial services. As regards implementation of the ECD, the FSA has held discussions with the European Commission, DTI and HMT, as well as with UK practitioner and consumer groups. Apart from clarifying the legal complexities, some of which have been mentioned above, the FSA is also preparing for the Directive's practical consequences. For example, the FSA (as well as the Financial Services Ombudsman and Compensation Schemes) will need to be able to respond to enquiries and complaints from consumers in other Member States, who are customers of UK based firms. The FSA will be assisting in the work of FIN-Net, the Commission sponsored network of alternative dispute resolution mechanisms,⁵ which will ensure that complaints are forwarded from the Member State where the recipient of a service is based to the appropriate national body in the Member State from where the provider of a service operates.

4 These tests are specified in Article 3(4) of the ECD.

5 Dispute resolution mechanisms in the UK include the Financial Services Ombudsman Scheme.

Other international fora

- B.12 The Financial Stability Forum (FSF).** This Forum comprises the finance ministers, central bank governors and lead regulators of the G7 countries. The FSA has played an important role in highlighting the need to look at the implications of e-commerce for financial stability. The international community needs to be able to monitor the challenges to the regulatory architecture in the fields of jurisdiction, supervision, enforcement, and consumer protection; to assess the adequacy of the responses to these challenges; and to determine whether fundamental changes to the world's regulatory architecture are called for.
- B.13** The FSA's assessment is that the existing regulatory architecture is currently able to respond effectively to envisaged levels of globalisation, provided that adequate systems are set up to ensure information is shared, that untoward events receive a timely response, and that regulators have powers to provide information and take co-ordinated action where required. This approach may be described as pursuing a policy of enhanced co-operation. The FSF has considered some of the issues which could potentially produce risks to international financial stability and as an initial step has established a Contact Group to take forward the FSF's work in e-commerce.
- B.14 International Organisation of Securities Commissions (IOSCO)** established an Internet Task Force in 1997 whose 1998 report made 24 recommendations, with which the FSA is compliant, including the adoption of the 'targeted at' test described in paragraph 4.12. The Internet Task Force has updated its 1998 report to take account of new market developments and is paying particular attention to five areas:
- a) the capacity, resilience and security of firms' computer systems;
 - b) liability for hyperlinks during the offering process;
 - c) day trading;
 - d) Internet discussion sites, such as bulletin boards; and
 - e) Internet enforcement and Internet service providers.
- B.15 Basel Committee's Electronic Banking Group (EBG)** is a sub-group of the main Basel Committee and comprises 17 central banks and bank supervisory agencies from the Basel membership, along with observers representing the European Central Bank, the European Commission and the bank supervisors in Australia, Hong Kong and Singapore. The EBG, which first met in November 1999, has focused on developing and sharing sound supervisory guidance and risk management principles and enhancing cross-border co-ordination among bank supervisors for e-banking activities.

- B.16 In June 2000, the EBG completed Phase I of its work plan, which included: two surveys of bank supervisors in the G-10 and selected non-G-10 countries on e-banking developments and the extent of supervisory policy responses in these jurisdictions; and regional E-Banking Roundtables for bank supervisors, financial institutions and service providers. It has published two reports, the first '*Risk Management Issues and Cross-Border Supervisory Considerations arising from E-Banking Developments*' and the second '*Risk Management Principles for Electronic Banking*' (<http://www.bis.org>).
- B.17 **The International Association of Insurance Supervisors (IAIS)** has recommended a set of three principles on the supervision of insurance over the Internet. Observance of these principles is at the discretion of individual IAIS members. These principles are:
- a) consistency of approach – the IAIS encourages its members to provide guidance on the circumstances in which jurisdiction will be asserted over foreign web-sites, and suggests that the 'targeted at' approach may be used;
 - b) transparency and disclosure – the IAIS states that supervisors should require firms to disclose basic information, including contact details of the firm and its supervisor and, details about how claims are handled, where to complain and the jurisdictions in which it can do business; and
 - c) co-operation – supervisors should make useful information available on their web-site, including contact details for other supervisors, a list of authorised firms, a hyper-link to the IAIS web-site.

Internal developments in the FSA

- C.1 The Internet and other web-enabled technologies present a number of other challenges for the FSA. These include ensuring a timely and co-ordinated approach to e-commerce issues; ensuring a timely and co-ordinated response to an e-commerce related crisis; staff training; and gathering and analysing electronic evidence for enforcement purposes. It also presents opportunities, including the use of software to facilitate surveillance of the Internet and ‘e-regulation’. ‘E-regulation’ is the use of the Internet and web technologies to improve the economy and efficiency of regulation through on-line interaction with firms. This annex outlines some of the action the FSA is taking.

Challenges

Timely and co-ordinated approach to e-commerce issues

- C.2 The FSA’s new Risk Assessment Division will provide the organisational and governance arrangements that will deliver a timely and co-ordinated response to e-commerce issues. This division will co-ordinate the task of identifying risks arising from e-commerce, working with risk units from other divisions across the FSA. Significant risks will then be prioritised and resources allocated to address them.

Crisis management

- C.3 The World Wide Web has created additional risks to the FSA, as well as to regulated firms and consumers. In line with industry best practice, the FSA regularly updates its crisis management procedures. The FSA has actively reviewed its procedures to take account of possible e-commerce related crises. The FSA liaises with government on relevant issues that are critical to the national infrastructure. The FSA is a member of the UK’s Information Assurance Advisory Council, and contributes to its goal of ‘building of a safe

and secure environment for e-Business, e-government and citizens in the 21st century’.

E-Commerce training

- C.4 Appropriate training for FSA staff can be a valuable tool for addressing a number of risks. Successful training programmes can effectively contribute to achieving all four of the FSA’s statutory objectives. There have been a number of training initiatives on e-commerce and IT issues. These have included briefings on the Electronic Commerce Directive (ECD), the Data Protection Act, Fund Supermarkets, the dot com phenomenon and the impact of the Internet on financial firms. The importance of keeping abreast of e-commerce and technological developments is recognised throughout the FSA and future training needs will continue to be identified and met.

Electronic evidence

- C.5 The growing availability of cheap computing and data storage is increasing the extent to which individuals and companies employ electronic means to store data. The capture and use of ‘electronic evidence’ can present new challenges to government agencies and regulatory authorities in respect of legal actions that might be taken on the basis of such evidence. The experiences of other agencies, such as the Serious Fraud Office, have provided useful lessons in this area. The FSA is taking steps to ensure that staff in its Enforcement Division have the necessary skills, IT tools, and legal knowledge, to enable them to capture electronic evidence effectively for the purposes of taking successful action against companies and individuals that act unlawfully under the Financial Services and Markets Act 2000 (FiSMA) and/or breach FSA rules.

Policing the perimeter

- C.6 The FSA intends to continue to undertake surveillance of the Internet to identify market abuse, breaches of the Listing Rules requirements, and perimeter offences. A variety of tools are currently deployed to monitor the Internet by the FSA. The FSA’s experience and that of other leading regulators is that existing tools are efficient and effective in some areas, but not in others. In particular, the FSA’s experience of ‘surf days’¹ is that they are heavily resource intensive. The significant human resources involved in undertaking occasional ‘surf days’ may be more effectively and efficiently deployed in the analysis and pursuit of the results identified by an automated search engine. The FSA’s adoption of this tool would be consistent with its

1 A ‘surf day’ is an occasion whereby a number of FSA staff, during a specified day trawl the Internet for unauthorised investment advice/advertising. In the case of IOSCO ‘surf days’ this is done internationally with a number of overseas regulators, but the FSA also carries out its own ‘surf days’.

new risk-based approach, and the FSA is currently considering whether the use of Internet related technologies, such as automated search engines and ‘crawlers’, similar to those employed by other regulatory authorities, would provide a cost effective solution. An automated search engine is, however, merely one tool that the FSA could deploy against abuses perpetrated through the Internet. Consumer education and an effective complaints handling mechanism are also important.

Opportunities

E-regulation

- C.7 The development of Internet related technologies presents opportunities as well as challenges to the FSA in its approach to regulation. The FSA is addressing the practical and technological issues associated with the use of the Internet as a key channel for interfacing with firms. Delivering Internet based interfaces requires that a robust infrastructure be in place and that applications are sufficiently flexible to serve the needs of both the regulator and firms.
- C.8 *‘Building the New Regulator – Progress Report 1’* stated: ‘The FSA is committed to taking full advantage of technology to improve efficiency, to analyse and understand markets better in order to obtain early warning of emerging risks, and deliver general information and advice to consumers. We are now turning our attention to systems which will enhance our efficiency. Our development programmes will start with urgent projects such as the electronic processing of approved person forms. In the longer term we will review the methods by which we currently capture regulatory data’.
- C.9 The publication of an electronic version of the FSA Handbook on the FSA’s web-site will mark a new approach to its dissemination of rules and guidance. In addition, the FSA is considering ways to enable users to customise their view of Handbook content, in order that only content relevant to them is displayed.
- C.10 The existing regulatory regimes and the new Handbook require firms to submit various types of returns. The approach to electronic submission has been varied across the existing regimes and the majority of correspondence between the regulator and the regulated is still by paper means. To meet its statutory objectives, the FSA should have regard to the most efficient and economic way of improving interfaces in this area. The collation and analysis of data through paper submission are inefficient and work is underway to ensure that more efficient processes can be introduced. The FSA has already made progress in this area through the development of the Pension Review

and Monitoring Division's extranet, which facilitates on-line web-based submission of data by the firms concerned.

- C.11 TARDIS will be the FSA's new internal database for regulated firms, individuals, and appointed representatives. It will also be used to process applications made by firms and individuals. TARDIS is currently being developed to facilitate the 'grandfathering' work that is scheduled to take place in the transition to the new regime. The next phase of this development is to extend the system functionality of TARDIS and build upon this strategic platform.
- C.12 In CP26 *'The Regulation of Approved Persons'* the FSA committed itself to launching a pilot programme on the electronic submission of forms for individuals. The FSA's Individual Vetting and Registration department (IVREG) currently receives in the region of 2,500 application, withdrawal, and change of details forms each week. It is important that these forms are processed in a timely and efficient manner. One way of increasing the efficiency of this process is to collate electronically the application details at source, i.e. from firms, and to feed that information directly into TARDIS. IVREG will, therefore, facilitate the submission of such forms by regulated firms over the Internet.
- C.13 If this pilot demonstrates the anticipated benefit to firms and the FSA, it is planned to introduce more such initiatives including electronic submission of financial returns using interactive validation, and enabling firms to amend their static data which is to be held on TARDIS. Streamlining processes in this way will result in greater efficiencies for firms and the FSA.
- C.14 The FSA's Central Register, which is accessible via the Internet to enable consumers to check if firms are authorised, will be enhanced to reflect the new and integrated TARDIS information.
- C.15 The FSA's Comparative Tables project will enable consumers to compare the features of certain products on the FSA web site. The FSA is currently considering how such services can be enhanced e.g. through the use of hyperlinks to authorised firms etc. (see chapter 8 for further details).
- C.16 The UK Listing Authority is currently developing a web-based system for firms to submit documents requiring approval direct to listing staff securely and quickly.
- C.17 Under the new Training and Competence Regime the FSA will undertake a programme of industry training in order to raise and maintain standards of competence within the financial services industry. The FSA aims to use industry training to help secure compliance within firms and to secure a clear framework of standards both domestically and internationally. Distance learning materials have an important role to play and a pilot programme will

be introduced towards the end of the year. The potential benefits of using the Internet in this area include faster communication, the ability to reach a wider audience, and greater interaction and two-way feedback.

- C.18 Harnessing Internet related technologies and increasingly adopting a strategy of 'e-regulation' carry benefits for all stakeholders in the regulatory regime. Technology enhanced processes and consequent increased efficiencies in the processing of data and returns from firms will release to other areas internal resources traditionally associated with these tasks. Other opportunities to enhance the methods by which the FSA communicates with firms exist through the use of e-mail and extranet links. Web content lies at the heart of the FSA's communications strategy and will play a key role in facilitating the achievement of the FSA's statutory objectives.

On-line finance consumer messages

- D.1 D.1 The Internet brings real opportunities for consumers as well as firms. It offers an additional way of accessing a range of financial products and services which can be quicker, easier and more convenient than existing delivery channels. However, it is important that consumers are adequately prepared for using financial information and services on-line, and are aware of the risks and how to reduce them. The following messages aim to help make the public aware of issues they should consider when undertaking on-line finance and to help educate consumers about ways in which they can reduce the risk that things might go wrong. On the following pages are the consumer messages to be published as a Consumer Update on the FSA Consumer Help web-site (<http://www.fsa.gov.uk/consumer/>) at the same time as this discussion paper.

CONSUMER UPDATE

E-commerce, online services and the internet

The internet has opened the doors to new ways of doing business known as electronic commerce or e-commerce, including new ways to access financial information, products and services. For many people accessing services online (on the internet) can be quicker, easier and more convenient than the ways they've used before.

But don't forget, whenever you do something new you need to check out the risks as well as the benefits.

This Consumer Update gives answers to common questions about e-commerce and using online financial services, plus tips for using these services.

[What financial services can I get online?](#)

[What's different about buying online?](#)

[What are the tips for using online services?](#)

[What are fund supermarkets?](#)

[What is account aggregation?](#)

[Further information](#)

What financial services can I get online?

Financial services you can get online are not all that different from the ones you might have usually used. For example, you can operate a bank account, get a mortgage, buy and sell shares or an investment product.

You can also find a lot of information on the web to help you make your financial decisions, even if you don't actually buy online. For example, many websites offer instant quotations or calculators to help you work out what your mortgage repayments might be. Later this year, the FSA will launch Comparative Information Tables on its website to help you compare financial products across the market when you're shopping around.

There are also some more specialist financial services online such as investment related services like fund supermarkets or account aggregation.

What's different about buying online?

What are the tips for using online services?

What are fund supermarkets?

What is account aggregation?

Further information

What's different about buying online?

Some things may work a little differently from what you're used to, or from what you expect. For example:

- You may have more passwords and other security information to remember.
- You may need to follow hyper-links between different web pages or to scroll down menus to access important information such as terms and conditions or, for investment products, the key features document.
- When you're on a firm's website, it may not be obvious where they are based.
- You may not be able to access the website sometimes. In some cases, this might simply be because the firm has taken their website down at quiet times for maintenance, or it could be because there are a lot of people trying to use the firm's website at the same time.
- You may come across things like chat rooms and bulletin boards which are internet sites where people exchange views and news, for example, on the stock market. This can feel friendly like talking in the pub but, as with chatting socially, the information is not always accurate or reliable.

What are the tips for using online services?

What are fund supermarkets?

What is account aggregation?

Further information

Using online services: tips

Shopping around

When you're looking for financial products and services in the high street you usually get a better deal by shopping around. The same is true of looking for products and services online. However, there are a few additional things you might want to add to your checklist for shopping around on the internet.

- Check out a number of firms, not just one.
- Before dealing with firms you've never heard of, check whether they're authorised.
- Have a clear idea of what you're looking for.
- Compare what you'll get, features and prices of products and services.
- If you're going to buy online or use a service online, consider how easy a firm's website is to use – how easy is it to find your way around? Can you find the information you need?
- Read the product details, terms and conditions, key features, etc before you commit yourself. And don't press send or click to continue until you are sure.
- Print off or save information because you may not get a paper copy sent to you. For example, print off the terms and conditions – they may have changed if you go back to the website later.
- If possible, print off forms you've filled in to keep for your own records – you may need them if you have to make a claim later.
- If you fill in forms online, check all option-choices you select – drop down menus may have default options already filled in which you might want to change. For example, the default might be an interest-only mortgage, but you might be looking for, and need to select, a repayment mortgage - check the default and look down the options for the one which is right for you.
- If you receive paperwork, check it when it arrives.
- Get in touch with the firm straight away if you find a mistake.
- Don't go ahead unless you are entirely happy with the service, deal, terms, etc.
- (Check out security and safety tips below).

Safety and security tips

The internet is a public network so it's important to take a few precautions to try and ensure you:

- Know who you're dealing with
- Check the connection between you and the firm is secure
- Keep your information private, safe and secure, for example, passwords and other security information
- Keep your computer safe from unfriendly software such as viruses

Know who you're dealing with

The vast majority of online financial firms are genuine and authorised firms. But it is possible for fraudsters to set up a dummy or look-a-like site so that they can try and get people to hand over banking details, credit card numbers and other security information. Check out the following if you're using online financial services:

- **Check that you've logged on to a firm's genuine website.** Some dummy or bogus websites may deliberately use a name or web address very similar to that of a genuine firm. Don't continue if you think there is anything odd about the website. Always check the web address you have typed is the correct one before providing your personal security information and carrying out a transaction.
- **Check that the website provides information which identifies the firm.** This should include a physical (postal) address and telephone number for the firm. Check this contact information using other sources, for example, Directory Enquiries or Yellow Pages.
- **Check the firm you're dealing with is authorised.** An authorised firm must meet set standards before they are allowed to do business. You are only protected by the UK complaints and compensation schemes if you deal with an authorised firm or its appointed representatives. Financial firms in any country in the European Economic Area (EEA) can offer products and services in any other EEA country – firms are regulated in the home country but must also meet standards which have been agreed across all EEA countries. To check if a firm is authorised call the FSA Consumer Helpline on 0845 606 1234 or check the Central Register directly at www.thecentralregister.co.uk.
- **Check the details of overseas firms.** The web's full name is the World Wide Web - and it is world-wide. You may find services offered by firms based in countries outside of the EEA. If you are thinking of doing business with an overseas firm, check if there are contact details so that you can find out how they are regulated and if there are complaints and compensation schemes.
- **Comparing information.** The internet makes it much easier to access products and services from different countries. When you're looking at information about products online, remember that not all information will be put together on the same basis and not all products will be directly comparable. For example, illustrations of what you might get back could be based on different assumptions about how an investment might perform, and different products could have different tax treatments in different countries.

Check the connection between you and the firm is secure

You should only provide bank details, passwords, PIN numbers, credit card details and other security information to firms that encrypt the data so no one else can read it. You can check the connection is secure by:

- Asking the firm if your transaction data is encrypted (in code so that people outside of the firm you are dealing with can't intercept or read what is being sent between you and the firm).
- Looking for the firm's security policy on the website to see if data is encrypted.
- Looking for a closed-padlock or other security symbol on your screen or 'https' in the left-hand side of the web address box (instead of 'http') to indicate encryption is taking place.

Keep your information private, safe and secure

Use your passwords and other security information carefully. For example:

- Choose your passwords carefully - don't use obvious things like your account name, date of birth, or the word 'password'.
- Try and ensure your passwords and other log-in details are unique and could not easily be guessed by other people.
- Try and memorise your passwords and other security information - try not to write them down (others might find and use them).
- If you do need to write them down because you can't remember them all, don't leave them where they can easily be found (e.g. by your computer) and don't write them down in the same place. It is also important to disguise them so it isn't obvious what they are for.
- Do not store your password on the PC, it's much safer to type in your password each time you access the service.
- Try to avoid accessing sensitive information in a public place - if you need to do so, whether at work, in an Internet café, a library, etc, make sure no one is looking over your shoulder at the computer screen.
- If you do access sensitive information in a public place, never leave the computer unattended and close down the internet browser program when you are finished to clear any security information from the PC.
- If you think someone else knows your security information, tell the financial firm you're dealing with straight away - when you contact the firm they'll tell you what to do.

The safest way to operate your online accounts is to keep your passwords and other security information confidential. However, some services ask you to let them know your password - if you want to use these services and you haven't checked with your original service provider that this is okay, you may risk losing money if an unauthorised transaction takes place. For example, account aggregation service providers may ask for your passwords (account aggregation services allow you to view all information from your different online accounts on one website). Always check with your service provider if it is okay to give your password to another service provider before using the services of the second provider - if in doubt, don't give your password to anyone else.

Keep your computer safe from unfriendly software such as viruses

A computer virus is a program that could stop your computer working properly. Some virus programs can record what you type, which could give them the information they need to access your online financial accounts. Viruses can be sent as files attached to e-mails. You can help prevent this by:

- Deleting e-mails with attachments before you read them if you don't know and trust the person that sent you the e-mail.
- Installing good anti-virus software to check for viruses before you open files – check out computer retailers and computer magazines for further information.
- Keep your anti-virus software up-to-date - new viruses are developed regularly, so keep up by downloading updates from the manufacturer's web-site.

What are fund supermarkets?

What is account aggregation?

Fund supermarkets

A fund supermarket is where you can buy the funds of a wide range of providers from a single site and hold them in a single account, often via the internet. The advantage is that within a single investment, such as an ISA, you can spread the risk among a range of funds and providers.

If you're thinking of buying from a fund supermarket, check out what charges you will pay on the funds – shop around for the best deal.

What is account aggregation?

Further information

Account aggregation

Account aggregation lets you see the information from all your online accounts on one website. This could include your current account, savings and investments, mortgage, credit cards and personal loans and reward schemes such as supermarket reward points or air miles.

Firms offering account aggregation will often take the information from other websites where you have accounts – this is called ‘screen scraping’. The firm operating the account aggregation service logs in as you and uses your security information, such as passwords, to get your information for you.

Experience in countries where account aggregation is already available shows some people wish to take advantage of this service – it can be a helpful tool in managing their finances more effectively. But there are also risks involved in disclosing security information such as passwords.

Before signing up with an account aggregation service, ask the following questions and consider how comfortable you feel with the answers:

- **If I give the account aggregator my passwords, will I break the terms and conditions of my other online accounts?** Check with the firms where you hold your online accounts – if you do break their terms and conditions you could be liable for errors or frauds on your account, however they occur.
- **How will the account aggregator use information about me?** It could be sold on to other firms for marketing purposes – check the account aggregator’s privacy policy before you join.
- **What steps will the account aggregator take to ensure my passwords and log on details are held securely?** Check on the account aggregator’s website what steps they have taken to ensure their systems meet high security standards – ask if you’re unclear.
- **If there is a security failure and money is lost, data corrupted or private information disclosed, who will be responsible for putting things right and compensating me for any loss?** Check out with both the account aggregator and your online account firms how they view their responsibilities in the event of something going wrong.
- **Do my online account providers allow account aggregators to log on to their computers to access and take my information (screen scraping)?** Check the terms and conditions of your online account providers – ask them if you’re unclear.
- **What happens if things go wrong?** Check with the account aggregator and your online account providers what they’ll do to sort out any problems which might happen. You may not have access to the Financial Ombudsman Scheme or the Financial Services Compensation Scheme.

Asking these questions will help you make an informed decision about whether you want to use an account aggregation service.

[Further information](#)

Consideration of .fin¹ as a tool of supervision

- E.1 This annex provides further detail of the FSA's assessment of whether it wished to pursue the sponsorship of a financial generic Top-Level Domain name² (TLDs) as a tool for mitigating risks to the FSA's objectives.

Mitigation of Risks to the FSA's Objectives

- E.2 The starting point in examining use of .fin as a regulatory tool was to identify which of the risks to the FSA's four objectives might be reduced by the use of .fin. The 17 highest priority risks identified by the theme (see Box 1 on page 26) were reviewed to assess which might be mitigated by the introduction of a regulator-sponsored TLD.
- E.3 The key identified risk was that significant financial crime occurs via e-commerce delivery channels. Were this risk to materialise, it would have an impact on the consumer protection, market confidence and financial crime objectives.
- E.4 **Consumer protection.** The use of .fin will help indicate to those consumers wanting to use the Internet to buy financial services whether they are dealing with an authorised firm, and possibly the country in which the firm is authorised. The use of .fin could help consumers identify more easily authorised firms and the extent of any redress that might be available in the event of difficulties, thereby improving their decision making. The risk of consumers unwittingly doing business with unauthorised entities is not insignificant – in two separate 'surf days' conducted by the FSA to search for Internet scams, action was taken in about 15 per cent of the 94 sites which were found to need further consideration.

1 In this paper .fin is used as a shorthand for the top-level domain name; thus the Uniform Resource Locator (URL) the global address of documents and other resources on the World Wide Web) for a firm using it would be xxxbank.fin, or if used to indicate country of origin, xxxbank.uk.fin.

2 Top Level Domain names are the final section of Internet addresses. There are two main types: country code Top Level domain names, e.g. '.uk', '.nz', '.fr', or generic Top Level Domain names, e.g. '.org', '.com'. This section focuses on generic Top Level domain names, which will be referred to in this section of the paper as TLDs.

- E.5 **Financial Crime.** A well-controlled .fin would not only increase consumer awareness about the authorisation status of firms, it would also make it easier for the FSA to police the perimeter, since unauthorised firms would be tempted to use a .fin address in order to promote effectively their scheme to investors, but regulators would find it relatively easy to identify an unauthorised firm using such an address.
- E.6 **Market confidence.** A reduction in the number of customers unwittingly doing business with unauthorised firms over the Internet would enhance confidence in the use of e-commerce delivery channels in the purchase of financial services both for consumers and other firms.
- E.7 Whilst risks to the achievement of the **Public Awareness** objective are not directly mitigated by the use of .fin, it may bring about greater public awareness of the protections that are provided by dealing with authorised firms.
- E.8 Thus, .fin would have potential both as a preventative tool (i.e. by giving a clear signal to consumers which sites are authorised to provide regulated financial services) and also, as a monitoring tool (i.e. helping enforcement to identify those who are undertaking authorisable financial services activity without the necessary authorisation).

Effectiveness

- E.9 The next factor to consider in deciding whether the FSA should use .fin as a regulatory tool is how effective the tool would be to mitigate the identified risks to the FSA's objectives. Assessing effectiveness will be determined by reference to four different categories: breadth; persistence; verifiability and timeframe. These are discussed in turn below.
- E.10 **Breadth** (*range of target groups that could be affected by tool use*). The use of a TLD as a regulatory tool would affect all the FSA's main stakeholders and possibly beyond:
- a) **Consumers.** The use of a .fin TLD as a regulatory tool would have benefits for all consumers who used or wished to use the Internet to buy financial services, by indicating the authorisation status of a firm and the country in which it was authorised. The use of .fin might also contribute to enhancing confidence in the use of these channels, and thereby increase the number of people benefiting from the use of e-commerce delivery channels.
- There are, however, other methods which the FSA could pursue to ensure it is clear to consumers which firms are authorised to offer regulated financial services, both on-line and when using 'physical' delivery

channels. One of the advantages of using a regulator controlled TLD is that it would be much harder to fake the authorisation required compared to, for example, a compulsory status disclosure on an authorised firm's site. .Fin could thus help foster higher levels of consumer trust.

- b) **Authorised firms and industry.** For firms, the risk of existing and/or potential customers falling prey to frauds committed via spoof sites may be reduced thereby increasing trust in the use of e-commerce channels. For the industry in general, the larger and more robust the e-commerce market, the greater the incentives for innovation.
- c) **Others.** If a country code indicator were used with .fin to indicate where the firm in question was authorised, the international regulatory community may benefit from being able to identify easily where firms which are targeting their jurisdiction are supervised. .Fin would thus help identify the 'targeting firm's' supervisor, should concerns arise.

E.11 **Persistence** (*how long will the effect of tool application last*). The use of .fin as a regulatory tool is likely to persist over a considerable period of time, at least as long as the current Internet addressing system is in existence. Arguably the effectiveness of this tool will become greater over time as it could foster understanding by both consumers and firms as to what the use of .fin signifies and, as importantly, what it does not signify. This would bring about a greater understanding of the implications of authorisation. There may also be a reduction in financial crime via the Internet as customers become less likely to fall prey to such scams, and thus they become less profitable for criminals to target.

E.12 **Verifiability** (*how easy is it to confirm the effect of tool application*). It will be difficult to verify the effectiveness of this tool and its effects may be variable. Some examples of measures of effectiveness following the introduction of .fin are: there is an increase in successful enforcement action taken against unauthorised activity on the Internet; the number of consumers falling prey to scams falls; and the use of e-commerce delivery channels to buy financial services increases. However, it may be difficult to isolate how much any change in these indicators might have been due to the introduction of .fin alone. Moreover, the measures of effectiveness of the use of .fin in each of the examples given above may be different. The mitigation of the risks to each objective may also vary.

E.13 **Timeframe** (*length of time required for tool application and effect*). The timeframe for the application of .fin as a tool is likely to be longer than 12 months. This would include the time to complete the ICANN application process (i.e. agreement with other supervisors of an approach in the application, possibly waiting for application process to be re-opened, at least

three months for the application process) and subsequent establishment of the administrations and release of .fin to authorised firms.

Costs³

- E.14 The next stage is to review the costs of using the tool. The costs are detailed below, split into costs to others, mainly focused on authorised persons, and then direct costs to the FSA.

Compliance Costs to Authorised Persons

- E.15 **Staff time.** The introduction of .fin to indicate authorised status would take up staff time in making the necessary changes to its firm's presence on the Internet, for example registering the change of name, creating links from 'old' URL to the new one, and developing promotional material to guide customers to the new URL.⁴ Legal work may also need to be undertaken to determine, for example whether there are any jurisdictional requirements raised by the introduction of .fin. Firms might also wish to lobby those administering a .fin.
- E.16 **Management time.** Board and senior management understanding within authorised firms of the use of .fin would be essential, since a TLD would indicate authorisation status and would require firms to decide how their Internet presence would operate in the future (for example if a country suffix were used with .fin, those firms with one site serving multiple jurisdictions may need to consider having separate sites for each jurisdiction).
- E.17 **Third party fees.** It is highly likely that the FSA, or whoever administered the scheme on behalf of the FSA, would charge a fee, at the very least to cover administration costs.
- E.18 **Other costs.** Authorised persons with existing web sites would be likely to undertake some form of promotional work to inform current and prospective customers of the change to their URL. The costs involved will be high for those firms which have already invested considerably in brand recognition of their existing URL. There may also be costs – in addition to the staff costs mentioned above – related to changes in web site design that may be necessary, for example for those firms which are selling multiple products over multiple jurisdictions via one site.

3 The FSA has taken the assumption that the application for .fin would be made as part of an international co-operative effort between national supervisors. This is for several reasons, the most important being that the FSA regards the use of .fin with a country code as being the most effective use of a financial TLD and this will be best achieved via international supervisory co-operation. Moreover, it is likely that financial services providers from many jurisdictions would like to take advantage of .fin and thus sponsorship by one country may be inappropriate. Finally, a successful application for a TLD would need to demonstrate it is global in application.

4 Uniform Resource Locator, the global address of documents and other resources on the World Wide Web.

Direct Costs to the FSA

- E.19 If the FSA did wish to pursue the sponsorship of .fin, it would incur the costs below.
- E.20 **Staff Time.** FSA's staff time would be used in the following ways:
- a) **Preparation of an application to ICANN.** This would involve: high-level co-operation with other international regulatory agencies in order to present a united application to ICANN, and to agree the modalities of subsequently administering .fin; arranging a working model of administering .fin in support of the application, for example whether the FSA would outsource the administration and if so, identifying a provider and negotiating provisional arrangements with it for the administration should the application be successful; drafting, in co-operation with others, the application to ICANN (specialist staff would be needed, for example lawyers, IT specialists); initial awareness raising amongst firms and consumers of the FSA's application and, possibly, lobbying efforts in support of application.

If the application were successful, further considerations would then apply:
 - b) **Administration of the TLD.** There are two ways staff time could be used here, depending on the model for administration of the TLD that the FSA chose to use. If it were decided to keep administration in-house, either new specialist staff would need to be recruited, or existing staff would have to be redeployed, so as to administer the release and the removal of rights and/or ability to use .fin. If it were decided to outsource the administration of .fin to a third party, FSA staff time would nonetheless be used identifying a suitable firm, drawing up service level agreements, monitoring performance under these agreements and continual liaison (for example for release and removal of the ability for a firm to use .fin).
 - c) **Public awareness raising.** The public's awareness would need to be raised prior to the introduction of the scheme. It would be important to ensure that authorised firms were fully aware of the implications of .fin and what would then be required once .fin was introduced (for example transitional arrangements etc). This might be achieved by FSA staff drafting a circular to senior management followed up by supervisory contact. There would then need to be awareness raising amongst the general public as to what .fin meant. Possible issues for consumers are discussed in paragraphs E.24 and E.25. This public awareness raising would take FSA staff time to devise and manage.
- E.21 **Use of facilities.** There would be use of the main FSA facilities for preparation of an application and awareness raising material. There may be the need for

new monitoring software for enforcement. Finally, if the FSA decided to administer the release of the TLD itself, it would need to obtain the necessary infrastructure.

- E.22 **Preparation of material.** As alluded to above, the FSA would need to prepare, or at the very least input into the preparation of, an application to ICANN of a regulator controlled TLD. If the application were successful, the FSA would need to prepare explanatory material for all authorised firms about the FSA's requirements regarding .fin. Publicity material would need to be prepared in order to raise public awareness of the use of .fin. There would also be the further costs of specialist help needed to formulate any awareness raising campaign, and possibly significant advertising costs.
- E.23 **Other.** These would be costs related to the application process, specifically a contribution towards, if not all of, the \$50,000 application fee to ICANN (this figure is based on the non-refundable application fee ICANN charged during the last round of applications). There would also be the cost of administering the scheme. The nature of these costs will depend on whether administration is kept in-house or outsourced.

Risks and other factors to consider

- E.24 As well as the formal toolkit analysis above there are other factors which the FSA would need to consider before using .fin as a regulatory tool. The key consideration concerns public understanding of what .fin does and does not mean.
- E.25 There are the risks to the attainment of all four of the FSA's objectives if something were to go wrong with, or were perceived to go wrong with, the use of .fin. For example, if there were a major Internet security breach at an authorised firm, or an authorised firm doing business on the Internet failed. These are examples where the FSA's administration of .fin would have been in order, but public perception of what .fin signified, i.e. guarantees of good site security and that a firm would never fail, may be different from the reality. Examples where the FSA could be argued to have failed in its administration of .fin would be if consumers did business with a faked .fin site, or if a firm's ability to use .fin was not withdrawn immediately after revocation of authorisation. The first set of examples have implications for the costs the FSA may need to incur with respect to educating its stakeholders as to what .fin does and does not mean; the second has implications for the costs the FSA would have to incur in enforcement and in the administration of .fin.
- E.26 The FSA may also need to consider whether some of the benefits of a regulator controlled .fin could be achieved by another body, most likely a private sector firm, administering .fin, or by the FSA controlling the sub-level

domain .fin (i.e. xxxbank.fin.uk), which could be applied for and controlled on a unilateral basis.

Conclusion

- E.27 The use of a regulator controlled top level domain name to indicate authorised status could help mitigate risks to three, if not all four, of the FSA's statutory objectives. Moreover, if properly administered and well understood, it could help aid the achievement of the FSA's consumer protection and public understanding objectives, and encourage greater use of e-commerce delivery channels in the purchase of financial services, with the potential benefit of better deals for consumers.
- E.28 However, in the view of the FSA, the costs of achieving these benefits appear to outweigh the value of the benefits themselves.⁵
- E.29 The FSA will continue to monitor developments in the use of top-level and sub-level domain names. Should circumstances change or new opportunities arise in the area of top-level domain names, the FSA will assess these using a similar analysis to that detailed in this annex.

⁵ The costs include the costs to firms to ensure compliance with the use of .fin, as well as the costs to the FSA, and the risk of causing more rather than less confusion for consumers using the Internet to obtain financial services.

Questions

Questions of particular interest to consumer groups are shaded.

4. International context

- Q1: Do you agree with this analysis and conclusion?
(See paragraph 4.7.)

Global co-operation is necessary to regulate a global medium

- Q2: Do you think the FSA's policy regarding globalisation and e-commerce strike the right balance in seeking to meet the challenges of this new media? If not, what do you think the FSA should be doing?

6. Approach to Information Technology (IT) risk management

Ensuring IT risk management is properly considered at a senior level

- Q3: Would awareness measures to disseminate FSA's expectations of senior management in this area be helpful? If so what measures would be useful?
- Q4: What are your views on making this responsibility more explicit in the high level standards in the FSA Handbook?

Clarifying FSA's expectations

- Q5: Would you welcome greater clarity of FSA's expectations regarding IT outsourcing? If so, in what areas?

- Q6: Would you welcome greater clarity of FSA's expectations in the area of IT risk management?
- Q7: Would further information / awareness measures be useful?
- Q8: Would further guidance in the Prudential and Conduct of Business Sourcebooks be useful? If so, what areas should be focused on?

Incentivising good / adequate IT risk management

- Q9: Are there particular amendments to content or process of the current e-commerce questionnaire that should be considered as part of this short term review?
- Q10: Are there other issues or suggestions that should be considered in the short term review?
- Q11: Are there amendments to content or process of the current e-commerce questionnaire that should be considered as part of this longer term review?
- Q12: Are there other issues or suggestions that should be considered in the longer term review?

Dissemination of good practice

- Q13: Has the FSA been doing enough in this area? What additional means if any should be used? What areas do you think the FSA should focus on?

7. Approach to Consumer Security

Introduction

- Q14: Are there any other differences that affect the security of on-line financial consumers compared to other non-financial on-line consumers? (See paragraph 7.4.)

Three IT security risks facing consumers

- Q15: Are the security precautions suggested above and in Annex D reasonable and realistic? Are there any other security precautions that consumers should take to safeguard important data? (See paragraphs 7.7 to 7.10 and Annex D.)

Improving consumer security

Promoting good password practice

Q16: Are these approaches to promoting good password practice realistic? Are there any other approaches which should be considered? What measures should firms take to encourage good password practice?

Protecting the computer from attack by software programs

Q17: Do these approaches to helping consumers combat the risk of malicious programs seem realistic? Are there any other approaches which should be considered? What measures should firms take to enhance consumer security in this area?

Avoiding dummy and fraudulent sites as well as those promoting scams

Q18: Are these approaches to helping consumers become aware of the importance of checking the authenticity of a web-site realistic? Are there any other approaches which should be considered?

Q19: What responsibilities do firms and regulators have in this area? Should the FSA encourage firms to conduct surveillance to ensure their site is not being spoofed or should it be left to the firm to protect their commercial interest, reputation and brand name?

8. Approach to information for consumers

Introduction

Q20: Are there any other characteristics of consumers which are relevant to this discussion paper? (See paragraph 8.1 and Box 3 on page 52.)

Q21: Are the risks identified here material and realistic? Are there any material and realistic risks which have not been identified? (See paragraph 8.7.)

Ignoring cyberspace

Q22: Should the FSA be doing anything more to address the risk that consumers might ignore the opportunities of cyberspace?

Global buying

Q23: Should the FSA alert consumers to the importance of considering the significance of potentially different levels of consumer, regulatory and legal protections available overseas? How effective do you think the options suggested would be? Should it be providing other sorts of information, or taking other kinds of steps to address the risk that consumers may not be aware of the consequences of obtaining services from firms based in other countries? How might the FSA do this?

Q24: Aside from differences relating to ombudsman and compensation schemes, regulatory (including accounting) standards, tax and the jurisdiction of courts and the law which they apply, are there any other regulatory or legal differences of a material nature about which consumers need to be aware?

Information and choice

Q25: Are there any other features which distinguish the Internet and other web-enabled technologies and which would need be taken into account when considering what information should be made available to consumers? (See paragraph 8.23.)

Q26: Do you think additional guidance is needed concerning the use of small screens, such as those on mobile phones? What do you see as the advantages and disadvantages of the approach put forward above? (See paragraph 8.26.)

Consumer understanding

Q27: What other key messages to consumers should be considered? (See Annex D.)

Hyperlinks to the FSA's web-site

Q28: Are there any other valuable benefits which consumers may derive from hyperlinks to the FSA's web-site?

Q29: Does the policy on hyperlinks seem reasonable?

Hyperlinks from the FSA's web-site

Q30: Should the FSA's Central Register of authorised firms contain the firm's web-address? Should the Central Register also have hyperlinks to the web-site of an authorised firm? If so, please give your reasons and say whether or not this link should be to its home page?

Bulletin boards and chat fora

- Q31: Do you believe that UK users of bulletin boards understand the status of information posted onto different discussion sites? Why do you hold this view?
- Q32: Do you believe that UK users of bulletin boards understand the different approaches followed by operators of bulletin boards? Why do you hold this view?
- Q33: Would drawing up a code of practice provide any additional benefit to users of bulletin boards? Since non-authorized firms operating bulletin boards would be free to ignore a code of practice, how much benefit would a voluntary code have? Might users of a bulletin board that complied with such a code place too much reliance on material posted there?
- Q34: Should compliance with such a code be a necessary requirement for authorized firms operating bulletin boards? Should authorized firms operating bulletin boards be required to disclose prominently on their site whether or not they comply with any such code?
- Q35: Should all firms (those authorized and not) be free to monitor their own stated compliance with any such code, or should there be provision for regular third party audit as a condition of being able to say that such a code is adhered to?
- Q36: Would a code based around such criteria improve public awareness and reduce the likelihood of misleading postings being made? (See paragraph 8.40 and Box 4 on page 64.)
- Q37: How onerous would compliance with such criteria be (please give details)? (See paragraph 8.40 and Box 4 on page 64.)
- Q38: Since operators of bulletin boards could voluntarily adopt the IOSCO criteria, what benefit would be gained by the FSA issuing a code of good practice? (See paragraph 8.40 and Box 4 on page 64.)
- Q39: Are there any other ways in which operators of bulletin boards might minimise the potential for their sites to be used to abuse regulated markets?
- Q40: What are the advantages and disadvantages of these approaches? Do you favour a strategy that is built around any particular approaches? If so, which ones and why?

Best buys and good decision making

- Q41: Does the FSA need to take any action to ensure that consumers make appropriate use of "best buy" programs?
- Q42: Is there any uncertainty over the dividing line between computer programs that facilitate the decision making process (and which are not subject to regulation) and those which provide advice (and which trigger an authorisation requirement)? If so, what are the products or situations which create that uncertainty? Are there any other situations in which the distinction between information and advice may be unclear?

9. Adapting the regulatory approach

Aggregation

Security issues

- Q43: Is this analysis of security issues reasonable? (See paragraph 9.9.)

Possible supervisory actions

- Q44: Are the tools the FSA has considered using in this context the right ones? Are there any other actions the FSA should consider in relation to aggregation services?

Electronic signatures

- Q45: How do you see the business to business and consumer to business markets for digital certificates developing?

Money laundering

- Q46: Should it be possible for an electronic signature supported by a certificate issued by a third party, which has complied with the non-face to face requirements set out in the JMSLG Guidance Notes, to be relied on by a relevant firm as evidence of identity, sufficient to enter into a relationship with the customer? Does this obviate the need for any further checks to be performed before an account is opened?
- Q47: Alternatively, might such a signature require only a reduced number of checks to be performed, for example a single check on the address for fraud purposes, or one check on an address and another on identity?
- Q48: If an authorised firm can rely on an electronic signature issued by a trust service provider in the UK for the purpose of entering in to a

relationship with a customer, should an authorised firm also be able to rely on such a signature where the certificate is issued by a trust service provider outside the UK? If so, should any additional checks be required, and, if so, in what circumstances?

Q49: What identity related attributes do you believe should be held in or to support the certificate?

Q50: Are there any other material risks arising from the use of electronic signatures that are related to money laundering or to the need to reduce financial crime?

Q51: As regards record keeping, what requirements and arrangements should there be to ensure that years or several decades later it can be shown that a signature had been properly established, and that it had been checked and found valid at the time of use? What services supporting such verification, if any, need to exist before the acceptance of electronic signatures is allowed?

Q52: Is the on-going integrity of a digital certificate as important as the identity checks when the certificate is issued?

The way forward

Q53: Are these objectives reasonable ones? Are there any other key objectives that need to be met? (See paragraph 9.38.)

Q54: Are there any other non-compulsory ways in which authorised firms could use electronic signatures and certificates for the purpose of entering into financial relationships in the confidence that they were complying with the money laundering regulations 1993 and FSA's money laundering rules?

Q55: Do you support the approach laid out above for ensuring that proper controls and procedures are put in place so that digital certificates of identity can be relied upon for account opening purposes? Could the approach be improved, and if so how?

Q56: Does this approach take sufficient account of the differences between the use of electronic signatures in the business to business and consumer to business sectors?

Q57: In order to ensure that authorised firms have time to develop the processes and controls suggested above, what would be a reasonable time-scale for drawing up guidance in this area?

Q58: How do authorised firms propose to address the risk that a customer does turn out to have been laundering money using an account opened on-line, despite operating whatever controls are recommended?

Authorised firms as providers of trust services

- Q59: Are there other key areas issuers should address? (See paragraph 9.44.)
- Q60: Are these appropriate tools for the FSA to use? What other tools might it consider adopting? (See paragraph 9.45.)
- Q61: What kinds of information, if any, would firms wish the FSA to provide to any accreditation agency, were there to be information sharing arrangements which aimed to reduce regulatory duplication on the part either of the accrediting agency or the FSA?

Using electronic signatures in the course of business

- Q62: Have firms considered how current operational discretionary powers possessed by authorised signatories will be mapped into the digital world?
- Q63: How are firms planning to maintain an audit trail of digital transactions carried out by staff or computers?

The use of electronic signatures by consumers

- Q64: What should issuing firms' responsibilities be in this area? What else could be done, and by whom, to aid public understanding?

Top-level domains (TLD)

Costs and Risks

- Q65: Is the analysis of the advantages and disadvantages correct? (See paragraphs 9.56 to 9.64.)
- Q66: Is the FSA's view of whether it wishes to sponsor '.fin' the correct one? Are there any other considerations that are not mentioned in this section or in Annex E that the FSA should take into account in its analysis of the use of TLDs?

ISBN: 0117044563

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7676 1000 Fax: +44 (0)20 7676 1099
Website: <http://www.fsa.gov.uk>

Registered as a Limited Company in England and Wales No. 1920623. Registered Office as above.