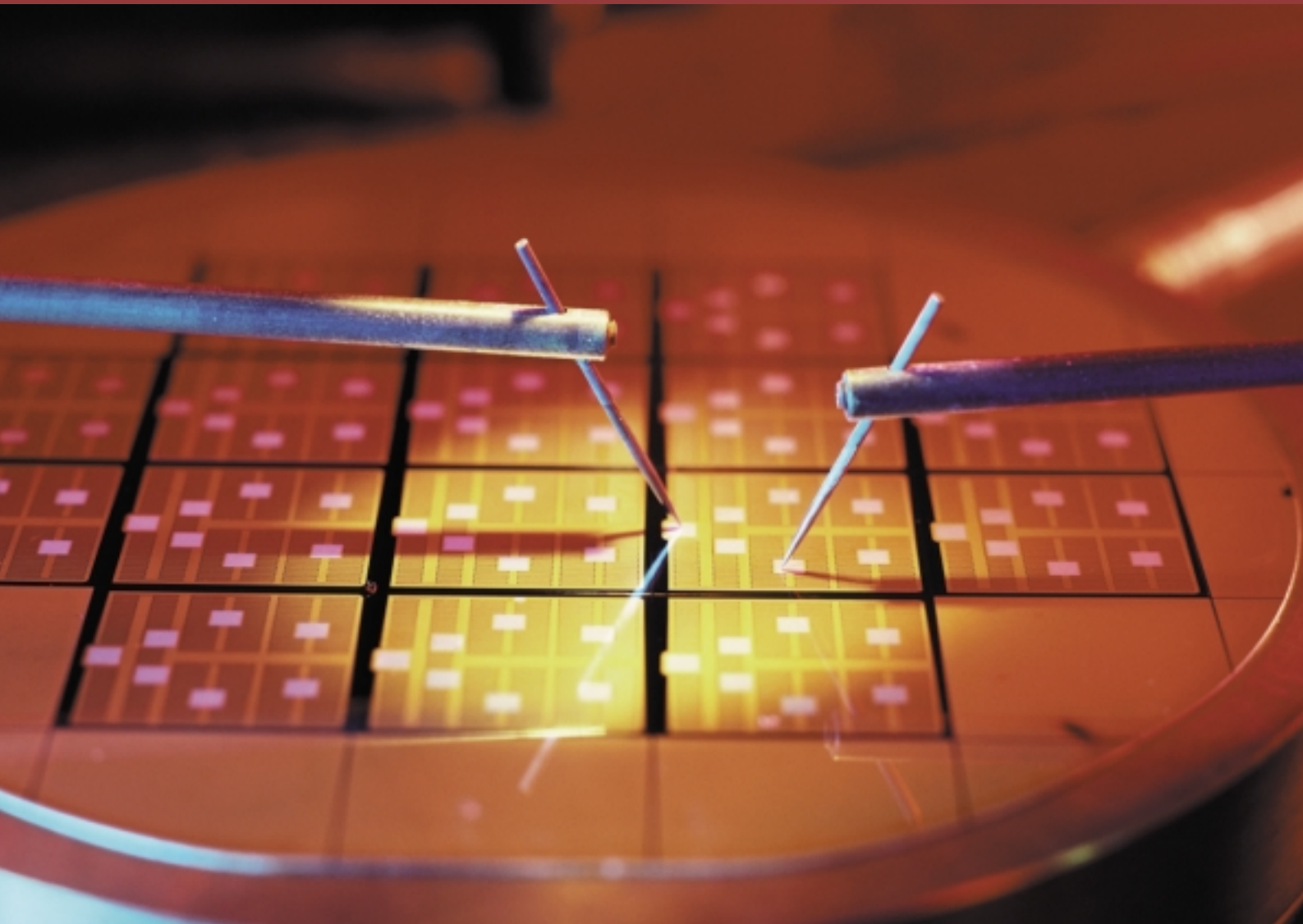
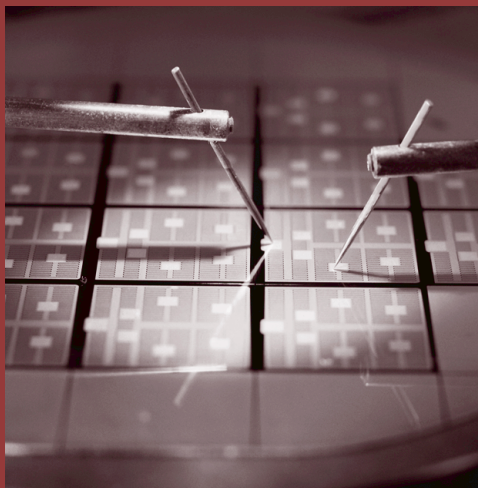


Protect and Survive

— Regulation of e-commerce in the financial services industry





Contents

	Page
Foreword	
Introduction	1
Executive summary	3
Key messages for e-managers and regulators	7
The phenomenon	9
The concerns and risk factors	19
How have the regulators addressed the challenge?	29
What are the future challenges for regulators?	44
The ball is in your court – the challenge to management	57
About PricewaterhouseCoopers	60
APPENDIX 1 To be in (e-)business tomorrow, what should financial services companies be doing today?	61
APPENDIX 2 Key global regulatory releases	65
APPENDIX 3 XML/ XFRML languages	68

Foreword

This paper represents a major contribution to debate on the regulatory and governance issues raised by the growth of e-commerce in the financial services industry. It has been written by two PricewaterhouseCoopers regulatory consultants based in the UK, Phil Gough and James Chrispin, with assistance and support from our regulatory specialists around the world including Bob Bench, Allan Schott and Roger Coffin in the USA, Rick Heathcote, George Stylianides, Sachiko Toki, Dominic Nixon and Jan Muysken in the Asia Pacific Region, Charles Ilako of our European regional team in Brussels, Martin Cornish from Landwell (PricewaterhouseCoopers' associate law firm) and many others. The authors have also benefited greatly from the advice and support of many financial services regulators and clients around the world.

The paper challenges firms and regulators around the world to build on their work to date in the development of greater global cooperation in the regulation of financial services delivered over the Internet, as well as encouraging them to undertake specific compliance and regulatory actions in each territory. PricewaterhouseCoopers will be delighted to support these initiatives with the objective of achieving the safe and secure growth for e-commerce in the financial services sector.

John Tattersall

Chairman of the PricewaterhouseCoopers UK Financial Services
Regulatory Consulting Group

Introduction

Background

Regulators do not have to, indeed should not, create the future, but rather they should respond in a timely and informed way to the demands of the public they serve. That public includes firms who want to reduce the expense of multiple regulation of the same activity, as well as consumers who by their individual purchasing decisions are in effect deciding, consciously or unconsciously, the particular regulatory system from whose protection they wish to benefit.

Traditionally, the responsibilities and jurisdictions of regulators have been determined and defined by national boundaries. The advent of the Internet with its unstructured environment requires a new response from the regulatory authorities:

'What we are seeing in the global e-business arena is not merely evolution, but revolution: a new way of doing business, driven by new technologies ... It is not only changing the way companies do business, it is changing the way we as consumers view the world. The new model is a boundaryless society with profound implications for where and how value is provided to customers.'

Jim Schiro, CEO, PricewaterhouseCoopers

- How do you regulate a transaction which takes place in virtual space?
- How do you identify and define a buyer, a seller, a transaction itself?
- How do you protect the consumer and their privacy when the currency of the Internet is information freely given?
- To what extent does the precise delivery medium affect the role and concerns of the regulator?

E-business is likely to transform several service-sector businesses, with the strongest impact expected in financial services. Rapid growth in web-based on-line banking, security brokerage, and insurance services has already been seen and is widely expected to continue over the next several years.

The financial services industry is ideally suited to the Internet and the pace of innovation has been challenging for the industry, and the regulators in particular. In a recent PricewaterhouseCoopers/CBI survey, 89% of respondents said that e-commerce was part of their current business strategy. In the same PricewaterhouseCoopers/CBI survey, financial services regulation and government regulation were both seen as significant barriers to e-business development.

This report

The purpose of this paper is to break down some of the uncertainty regarding regulation in cyberspace and to encourage progress in addressing the regulatory implications of e-commerce within the financial services industry. Things change, and fast. By examining at things as they stand, we explore the regulatory and consumer threats and opportunities offered by the Internet and look to identify the possible regulatory mandates and models of the future. This

'There is no doubt in my mind that we are in the middle of an explosion of Internet activity. We have to find a way of adapting our regulatory environment to new technology, not adapting the new technology to the old regulatory rules. The Internet helps the regulator, just as it helps the investment firm, bank or share promoter but we will need to have a fully worked-through strategy to exploit it...'

Sir Howard Davies, UK Financial Services Authority Chairman, September 1999

should serve as a preliminary guide to how business can prepare itself for the inevitable changes to regulation going forward. A competent e-business should be building these concepts into their new business designs now.

Specifically we examine:

- Threats and opportunities for regulation in cyberspace
- How regulators have responded to date
- Future challenges for regulators
- Future challenges for the industry

Scope of this report

In the e-business financial services arena, some would argue that the process of change has only just begun. Future technological advances such as WAP and other 'mobile-commerce' (m-commerce) applications may well raise new regulatory issues which will require continuous consideration by the regulators and regulated. This paper examines the issues surrounding mainstream Internet usage as it is today. With that background, the conclusions reached in this paper should be viewed as the initial findings of an ongoing study.

These issues apply to both existing market players that have adopted e-business strategies and newly created companies. Although in the main the issues facing these two groups are similar, where there are differences we have highlighted them.

The findings and conclusions of this paper are the products of our own internal and external global research and discussion, based on our understanding and experience of both Internet technology and the financial services industry. We are grateful to those who have made time available to discuss these issues with us.

Should you wish to talk to any of our specialists about the impact of the Internet on your business or explore your e-commerce strategy, you will find the names of a selection of PricewaterhouseCoopers regulatory specialists in the contacts section at the end of this document.

Executive summary

Regulation of financial services in an on-line environment is characterised by uncertainty. Whether it be determining whose rules apply, how they apply to e-commerce, how the regulators will approach the supervision of on-line delivered financial services or, indeed, how any of these factors may change as the market develops – thinking is embryonic, guidance is patchy and precedence is minimal.

The industry craves certainty without increasing the burden of regulation, and we have identified a number of areas where concern exists and/or action is required.

Global financial services businesses are concerned by the lack of consistency in the different regulatory frameworks around the world. Regulators must strive for common standards and approaches at a global level so as not to create a global imbalance in innovative uses of the Internet.

Jurisdictional boundaries are still seen as a major impediment to e-commerce business as they create uncertainty in terms of both contract law and financial services regulation. Failure to break down these barriers, or create safe harbours, and agree on globalised standards for the industry will result in e-commerce businesses having to put barriers and firewalls around the technology to insulate products and services aimed at one market and one set of market players from those aimed at the rest of the global marketplace. Some legislators have started to address the jurisdictional difficulties, although these are still at the highest level of concern for the industry as it seeks to develop the use of global Internet activity.

Global financial services businesses are also concerned that there is little coherence in the different regulatory frameworks around the world. Regulators must strive for compatibility and consistency between approaches at a global level if the innovative use of the Internet in financial services is not to be stifled. This is a huge challenge and one where there are no easy answers. However, the effort being made in enforcement and law agency co-operation is disproportionately greater than the effort being made to allow legitimate financial services providers to access the global marketplace and this requires redress.

To succeed in the information age, the e-business must build trust as this increases confidence, reduces inhibitions and barriers and hence allows people to transact business more freely. Excellence in information technology is key to this being achieved.

The financial services industry can avoid excessive regulatory scrutiny – and generate significant buy-in by consumers – by setting itself high standards in IT capability and effectively implementing these through a process of self-regulation. It is for each organisation to implement appropriate infrastructure to enable trust to be established, and it is for the regulators to demand the policies which will ensure that trust is not abused. Consequently, regulatory reform is likely to revolve around striving for excellence in IT to ensure high availability of services, thus protecting confidence in the markets and achieving confidence in the security and reliability of electronic delivery systems.

Where financial services companies are providing services over the Internet, regulators are increasingly seeking satisfaction that firms are managing risks properly. It is vital, therefore, that the financial services industry sets itself high standards in IT capability. This means appropriate planning, testing and implementation of IT systems.

The regulators must have the technology as well

Not only can Internet technology be used as a means to improve compliance monitoring within regulated firms, but it can – and, indeed, will – be used to improve supervisory processes within the regulatory bodies themselves.

The more forward thinking regulators have already started to incorporate technology-based monitoring into their supervisory activities through the application of compliance software, the receipt of 'real time' information and the use of the Internet for correspondence and regulatory reporting.

The majority of information received by regulators is historical, usually focused around month end returns. Specialist tools can now be developed, using the new generation of Internet languages, to receive and monitor 'real time' or near 'real time' data and to identify trends or exceptions. Such tools can be automated to a very high degree. In the medium term, these will offer a powerful regulatory tool to monitor an individual company's compliance with certain rules in 'real time'.

It is important to get the partnership right between regulators and regulated firms so that the Internet is a monitoring tool which also, subsequently, provides a gateway to regulators for supervisory purposes. However, 'real time' monitoring more generally could lessen the cyclical reporting burdens and constraints for companies, reducing the need for inspection visits and audit reviews.

Financial services businesses must anticipate these developments by improving their own on-line internal monitoring. Therefore, if and when on-line monitoring does arrive, they will be fully able to operate effectively in this new environment. This has the added benefit of enhancing the effectiveness of internal regulation, with knock-on benefits for the company's reputation, client relationships and regulatory relationships.

Concerns and risks

Time to market is often critical for on-line financial services businesses. Speed should not, however, be at the expense of prudent management of the business and executives should satisfy themselves that new on-line businesses have the necessary infrastructure in place and that they themselves have the competence to manage an e-business.

There is increasing evidence that newly conceived on-line businesses are being taken to market more and more quickly due to competitive pressures. But, do these new on-line businesses have the necessary infrastructure in place? In other words, are there appropriate middle and back-office and compliance functions to monitor, support and service rapidly built front-end operations? Management should challenge their collective knowledge and experience, taking action where necessary, to ensure that sufficient executive competence exists to understand and manage the issues and risks arising from e-business. Experience of successful management of an existing bricks and mortar business is unlikely to be sufficient in this respect.

New entrants themselves potentially pose the greatest risk. Technology is breaking down barriers to entry into the industry and challenging traditional methods of conducting investment business. Major new global industry participants have already appeared and, in the US, where the Internet market is more advanced, there are now large financial services businesses built purely on the back of on-line activity. This trend is likely to continue to bring greater risks and regulatory challenges, as the number of new entrants increases and the relative experience in the industry decreases.

The management challenge also exists in current businesses adding an on-line capability to an existing service, which do not have to endure a long drawn-out authorisation process. It is essential that the IT capability is properly managed – and there are plenty of cases where this has not been the case – but what about after-sales support and compliance? Increasing volume, for which the Internet is a catalyst, puts pressure on risk management and settlement functions and it is essential that these parts of the business are equipped to deal with these challenges. Equally important is the compliance function which must deal with new issues and challenges in the on-line arena as well as developing updated monitoring techniques. Such techniques must ensure that ineffective and antiquated practices are not being relied upon to support new, faster and cross-border delivered services. We believe that compliance software has a major part to play in the competent on-line financial services business of the future.

Systems downtime is one of the biggest risks for consumers when transacting with an on-line provider. Without effective business continuity planning, both consumers and the industry face the risk of financial loss.

Accessibility of services is absolutely vital in all areas of the financial arena. For example, an e-bank, which cannot maintain services to customers because of unreliable systems, is of no more use than a traditional bank without branches. Similarly, an on-line stockbroker or exchange that cannot display prices is failing in a critical area of its responsibility to members or customers.

Lack of service is not just inconvenient – it can cause actual financial loss, particularly where consumers are reliant on an on-line trading system. This provides further evidence, and a specific example, of the need for systems competence and an effective IT strategy.

Other significant risks faced by the consumer in an on-line world are the issues of privacy, suitability, the increasing evidence of an information and expectation gap and fraud. Any lack of regard for these in future regulatory policy may lead to financial loss to the participants in this industry, as detailed below.

Privacy: Due to the global nature of the Internet, information is transmitted across many borders and jurisdictions. If companies on the Internet are to gain the confidence of customers and, indeed, if governments wish to see the success of this phenomenon, protection of users, in particular with regard to privacy, confidentiality and anonymity should be assured.

Suitability: Concern stems from the fact that data profiling of customers, based on on-line behaviour, is being used by online brokers to make recommendations that may not be 'suitable' to the customers' financial situation, objectives and needs.

Information gap: Aggressive advertising has fuelled the misconception of easy wealth and the risk of being left behind in the new on-line era. Therefore, financial institutions must ensure that they are providing information to customers that is clear, user-friendly and not misleading.

Fraud: The Internet increasingly puts investors at risk through exposure to cyber-crime, mis-selling and direct marketing of unregulated financial services.

Future Challenges

Regulatory development is likely in three key areas: conduct of business and market conduct rules, prudential supervision and compliance monitoring and supervision techniques.

Conduct of business and market conduct rules: The greatest challenge in terms of rule making certainly applies in the retail sector, where conduct of business rules have been drawn up essentially to cope with the pre-electronic age. Regulators throughout the world are already addressing changes needed to the conduct of business rules, but there is a long way to go in terms of considering what notifications, risk warnings, 'reasons why', projections, cooling-off periods and suitability requirements should apply in respect of transactions through the Internet.

Equally, the use of artificial intelligence to respond to investors' queries and applications presents a further challenge to ensure that those artificial intelligence systems are adequately programmed and regularly updated to take account of developments in the market.

Prudential supervision and compliance: Regulators have always been concerned about risks other than purely financial risks such as credit and market risk. It has long been a requirement that financial firms should have adequate systems and controls. However, firms and regulators are now specifically

developing tools to capture the risk of financial loss that such risks, including operational risk, create. The dependency on IT systems, which e-business can only exacerbate, is a source of such risk.

Electronic reporting and monitoring: The regulators are already looking at ways of utilising the speed and flexibility of the Internet for monitoring purposes and the regulated community should be doing the same in order to enhance existing monitoring programmes and to ensure that their own e-commerce activity is monitored in the same way as other activities.

Fundamentally, however, the Internet is a new means of distribution rather than a new marketplace – consequently, in terms of the way that regulators regulate, the existing body of regulation is valid and applicable, and the need for specific regulatory rule changes is minimal. Action is required on the governance of firms in the industry, as explained above, which will be addressed most efficiently by the industry itself.

Consumer education is increasingly seen as a vital regulatory tool in the effort to ensure consumers receive the same level of protection in an on-line environment as they do elsewhere. The industry has a stake in this issue and should take further responsibility for ensuring that its clients are properly equipped to buy on-line.

The current focus of many retail regulators is ‘policing the perimeter’ rather than changing the way that legitimate Internet activity is regulated – keeping the wrong people out rather than looking at what people are doing ‘inside the fence’. The regulators’ tactic of choice, which we support, tends to be consumer education – to equip consumers with the knowledge required to buy sensibly over the Internet. The regulators and the regulated alike should accept responsibility for consumer education more widely. Investors should be:

- Equipped to differentiate between reputable and disreputable financial services providers
- Encouraged not to make spontaneous investment decisions
- Provided with sufficient information to make informed investment decisions
- Enabled to identify who they are dealing with and whose regulatory protection they can rely on

There is increasing evidence that the industry is taking responsibility for consumer education. More needs to be done, however, which might include industry funding of education in this area – even to the extent of hyperlinks to regulators’ web sites or to technology that gives relevant warnings. There is also commercial benefit to the industry – a well advised customer buys sensibly and will return – repeat business is key in this market.

Key messages for e-managers and regulators

In this section we draw on the results of our research. We propose specific action that the management of competent financial services e-businesses and the regulatory bodies themselves should be considering.

- **CEO / Directors generally**
 - Manage the activities of technical innovators and entrepreneurs in the business to ensure that newly delivered on-line businesses have the benefit of prudent management and supporting infrastructure
 - Integrate the role of the IT Department into the firm's regulatory and compliance control procedures as IT has a key part to play in delivering compliant services and satisfying regulatory requirements in the new electronic world
 - Review and challenge the composition of the board on a regular basis to ensure the necessary skills exist to effectively manage new products and businesses
 - Ensure the responsibility for innovative IT and back-office strategy is effectively delegated and monitored
 - Encourage regulators to take the actions detailed below.
- **Compliance Directors**
 - Ensure that all e-commerce projects/initiatives have appropriate compliance representation and support
 - Manage innovation within the compliance function to ensure that monitoring and control processes are keeping pace with, and are effective in supporting, front-office delivery
 - Take responsibility for shaping the approach to the regulation of e-commerce activity through lobbying and consultation processes. Regulators are looking to the industry to participate in the debate and this creates unprecedented opportunities to affect the development of policy, and enormous risk if the industry's constituents remain on the sideline.
- **Marketing Directors**
 - Work closely with Compliance to ensure that marketing and advertising initiatives comply with best practices, particularly with regard to suitability and privacy issues.
- **Operations Directors**
 - Ensure back-office functions including compliance, risk management and settlement are geared up to monitor and support on-line delivered services. The Internet has, in a number of examples, been a catalyst for highly increased trading activity and volume. The on-line share dealing world is a prime example of this. The key here is 'after-sales' management where credit risk and settlement processes are placed under huge pressure creating pressure points of systemic risk.
- **IT Directors**
 - Set high standards in IT capability and effectively implement these through a process of self-regulation
 - Devise and implement strategies that address the key risks in conducting financial transactions in an e-commerce environment. Such plans need to recognise the following three stage process:
 - Establishing trust
 - Ensuring security
 - Delivering operational governance
 - Ensure sufficient investment is made in maintaining IT integrity through capacity and systems upgrades

- Devise a reporting system to clients covering systems performance. This will have the additional benefit of supporting advertising initiatives assuming, of course, that systems performance is good.
- **Regulators**
 - Initiate and facilitate global co-operation in on-line regulatory requirements and strive for common standards and approaches
 - Use technology to improve existing regulatory processes
 - Devote resources to address new regulatory rule issues arising out of e-business and provide the industry with certainty in terms of interpretation
 - Channel further resources towards building on existing consumer education initiatives. These should include:
 - Educating investors themselves through, for example, their own web-based initiatives.
 - Defining disclosure requirements for the industry in terms of systems performance, regulatory status and product information.
 - Reviewing the advertising activities of member firms and proposing compliant frameworks for the advertising of on-line activities.
 - Working with the industry to initiate additional industry funded education campaigns.

The phenomenon

In this section we look at the explosion in on-line activity and give examples of current e-business activities in the financial services sector.

The main driver behind e-commerce activity is the Internet. Use of the Internet has, in many financial services arenas, become a key competitive parameter for long term success. Headlines such as these have become common place:

Rapid rise in on-line share trading expected to continue

Bond markets feel impact of e-revolution

Internet threat to traditional firms

The issues

The following key issues have arisen from the impact of the e-commerce revolution on financial services businesses:

- Changing the way in which consumers transact business with financial institutions
- Providing opportunities to re-engineer or outsource core business processes and functions
- Increasing both efficiency and service standards and potentially reducing costs
- Creating opportunities to re-engineer business-to-business transaction flows and processes
- Enabling new forms of money transmission or value exchange
- Creating new 'e-business communities' and trading relationships between manufacturers, suppliers and their respective customers.

We have analysed these points in four areas which are discussed in more detail below.

Convergence

Companies have converged to form cross-industry supply chains that have created fully networked markets and organisations. Businesses have converged with other businesses both within and outside the financial services industry. These new, dynamic, customer-centred networks may exist for only a single contract, a single customer, or a single instance. Customers gain convenience and choice, while firms benefit from being part of an extended, cross-industry value network.

The impact of technology is to allow businesses previously separated by industry sectors or geographical boundaries to form joint initiatives (see Figure 1.1). A prime example is the consolidation of European stock exchanges because the web allows cross-border penetration. There are numerous examples of convergence between the telecoms and financial services sectors, particularly for share dealing transactions, using a web-based infrastructure. In the UK, Abbey National unveiled cellphone banking partnerships with the Carphone Warehouse and Orange, and pledged to link with every UK mobile network. In Asia, Celestial Asia Securities in conjunction with Smartone (one of Hong Kong's leading cellular phone operators), developed the SmarTrade mobile telephone trading system.

The SmarTrade system operates on the basis of Short Messaging Service technology and offers a range of relevant financial information, such as index levels, bid-offer prices and trading volumes. The services can also be accessed from overseas. Two major Scandinavian banks, Nordic Bank and SEB Group, will soon offer wireless banking to a substantial number of customers using technology from Tantau Software Inc., a Compaq spin-off.

Some banks have considered or are actively considering strategic alliances or business partnerships with IT companies to explore business potential in the business to business ('B2B') markets or to leverage their expertise or resources in developing e-commerce or e-banking initiatives. Banks provide marketing through customer relationships whereas IT companies provide technical expertise and resources. For instance, four small local banks in Hong Kong have recently announced plans to form a joint venture with an e-commerce service provider to develop a common platform for providing e-banking services to their customers. Another local bank (Bank of East Asia) and Yahoo have also recently launched a co-branded web-site.

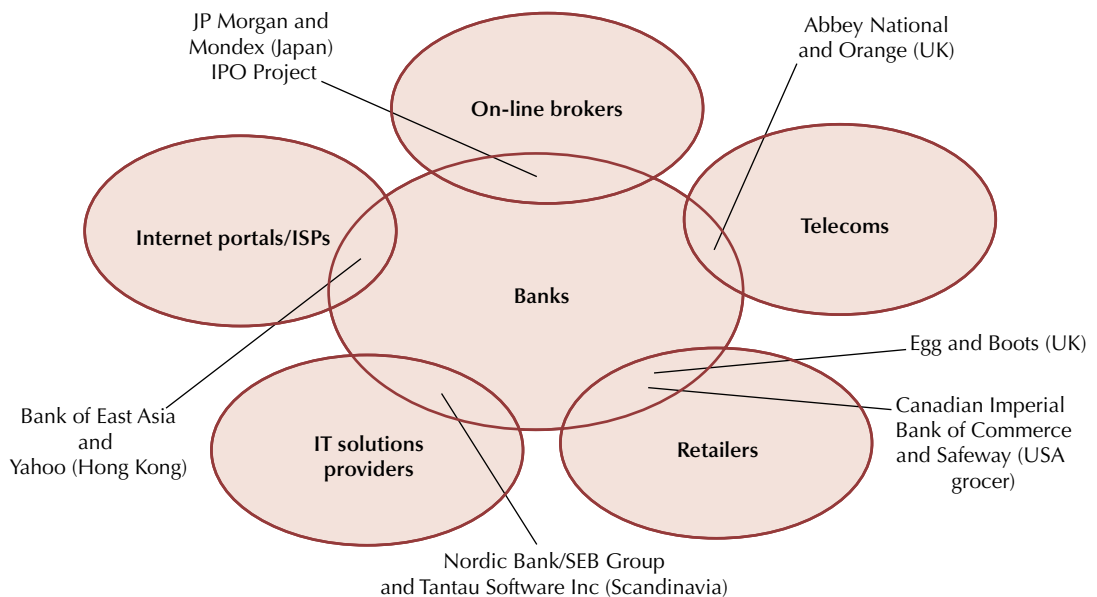
As a result of convergence, financial services companies are ceasing to brand themselves purely as banks or stockbrokers, but as fully fledged Internet companies. An example of this is Egg in the UK, which does not use bank as part of its company title.

Financial services companies are also creating financial services portals which sell branded products from a range of different providers. This promotes the phenomena of strategic alliances between web information providers and financial services companies. These portals are also likely to include more and more non-financial information as they grow in popularity, further blurring the boundaries of branding as a bank or as an Internet portal.

To assist with convergence plans, consolidation via merger or takeover is often seen as a swift route to form cross-industry links. Examples of consolidation are numerous including recently, in France, a takeover by BNP of Banque Paribas. In the Far East, players such as SoftBank are acquiring vast financial empires covering all aspects of e-commerce and financial service activities. In Latin America, Mexico's second largest bank agreed to be taken over by Spain's Banco Bilbao Vizcaya Argentaria.

The lowered barriers to entry in the marketplace have also encouraged businesses to practice divergence,

Figure 1.1 - Industry convergence: already happening, but easier in cyberspace



the opposite of convergence. Financial service companies have set up Internet sites in areas that are distinct from their traditional service lines. For example, building societies have set up Internet banks in the UK, recognising the possibility of cutting costs by avoiding the need for a large branch network.

Disintermediation and lower costs

The process of disintermediation is the elimination of value added costs of the intermediaries by providing wide access for trading commodity products, leaving the traditional intermediary to engage in sophisticated value-added services.

The Internet has made financial products more accessible than ever before, linking buyers to providers directly through financial supermarket sites. A striking example of this phenomenon is the massive boom in on-line share dealing, which has been made accessible to the public at a lower cost than ever before. The lower costs of starting an e-business have also eroded the traditional barriers to market entry.

Therefore, new players are emerging and strategic opportunities are created for financial services companies to form alliances with technology and commercial partners. New vendors in the United States, such as E-Loan and Lending Tree, are winning market share for certain products, resulting in the commoditisation of banks' key products.

The 'me-too' factor

Large investment and retail banks are being driven to set up initiatives to gain the support of analysts and investors. Traditional business models which were once the core strengths of businesses, whilst not obsolete, are diminishing. Share prices of companies which do not demonstrate that they have adopted a viable e-business strategy will fall against other key competitors.

Therefore, in already congested markets such as retail banking, many Internet banks are being created so that companies are perceived to be progressive in their business strategy-making decisions. In some markets this has led to overcrowding and the long-term implication must be that there will be a shake out of the least competitive players.

Cannibalising the customer base

It is inevitable that a large growth in Internet products will lead to customers leaving their existing high street outlet for a 'clicks and mortar' or 'clicks' only outlet. At many banks, customers are leaving their existing branch to emigrate to the Internet branch. This is, in effect, cannibalisation of the customer base by moving them from one transaction media to another.

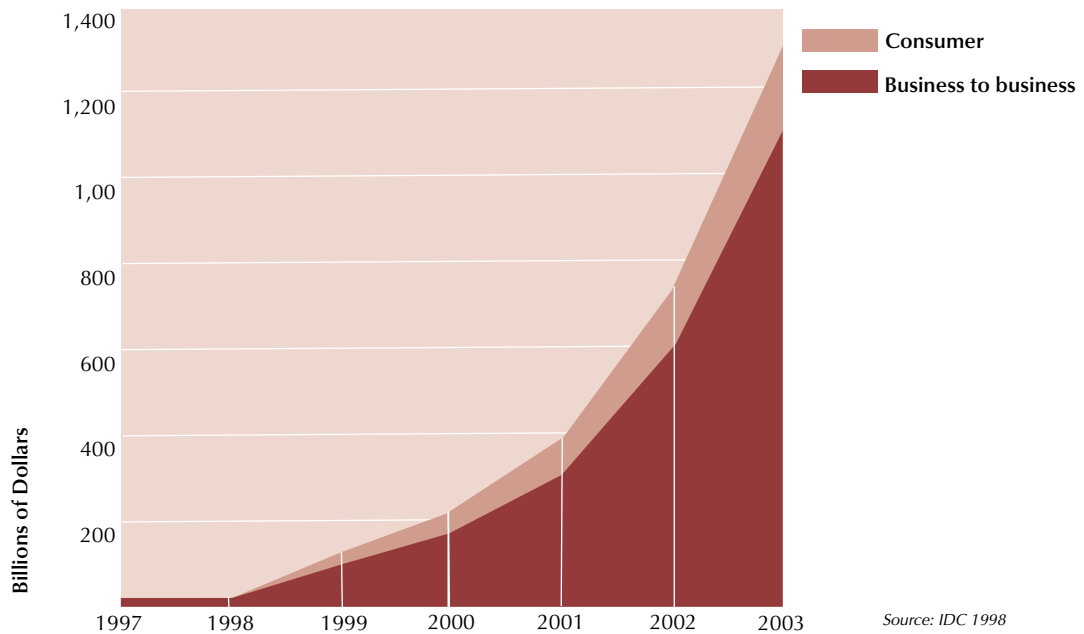
Industry sector analysis

There are a variety of regulated financial services offered over the Internet which can largely be broken down into business-to-business and business-to-consumer activities.

Whilst press attention has focused on the business-to-consumer arena, the trading volumes are far larger in the business-to-business domain. Current estimates are that business-to-business transactions accounted for 76.8% of all on-line sales last year and it is predicted that this percentage will grow to 85% by 2002. Therefore, it is clear that the most important market in terms of revenue, though not necessarily the most high profile, is the inter-business sector (see Figure 1.2).

Below follows an analysis of the type of activities that are occurring within financial services in these two areas.

Figure 1.2 – Worldwide commerce on the web



Business-to-consumer ('B2C')

Business-to-consumer activities have received the greatest attention, most noticeably in the on-line broking and banking markets:

Securities

This sector comprises on-line brokerages including information, execution and portfolio management. Other securities based sites offer investment intermediation supermarkets or act as information providers with corporate news, advice and information.

Probably the most significant trend in the securities markets today is the increase in competition due to the rise of new market participants – on-line brokers. On-line brokers empower investors by giving them more choices and more information. This revolution has been led by the US where, in 1994, there was not a single broker on the Internet. Today, there are over 160 broker-dealers on-line, accounting for more than one-third of retail customer trades. In Europe, the number of on-line trading accounts will grow from 1.85 million to 16.8 million by 2003 (May 2000 – IDC).

These entrants have increased access for investors by offering lower prices for services. Commissions for on-line trades have dropped about 70% over the past two years, from around \$53 to as low as \$8 in the US and \$12 in continental Europe (FT 26/06/2000).

In the UK, on-line share dealing more than doubled in the last quarter of 1999 rising to 371,000 trades in that period.

In the US, volume has increased from under 100,000 trades per day in 1996 to well over half a million by the second half of 1999.

Technology has brought with it greater competition and new marketing opportunities. Asset gathering, data mining, and cross-selling have become the common strategies of choice in competition for market share from individual investors. Technology has developed to the point where diversified financial firms can

develop highly sophisticated customer profiles based on past observed behaviour, combine it with transaction history, and deliver highly personalised information to their customers.

On-line trading activity is not limited to equities. Debt has also taken to cyberspace with the advent of e-offerings leading to predictions of a transformation in the bond markets. The primary market has seen a flurry of issues marketed and launched via the Internet directly to retail and professional investors.

Banking

Securities trading is only one area of the financial services sector being redefined by e-business. In 1998, more than 1,200 banks and credit unions in the US signed with on-line banking application vendors and providers to build fully transactional web-sites. In 1999, 7,200 banks and credit unions were expected to acquire on-line banking applications, a 500% year-on-year increase in the number of institutions investing in on-line financial services technology. In the US, there are nearly half the world's estimated fifty million current on-line banking customers (Angus Reid 20/06/00).

Most banks offer undifferentiated services such as interest rate information, FX transactions, balance and transaction inquiries, funds transfers, bill payment, time deposit services, on-line loan applications (including mortgages, personal loans and credit cards) and other miscellaneous functions (e.g. statement/cheque book request, financial calculators/analysis tools). Some of the banks also provide on-line stock broking services to their retail customers.

Some banks have also started initiatives to establish 'stand-alone virtual banks', which would deliver banking services predominantly, if not entirely, through the Internet or other electronic delivery channels.

Account maintenance on-line and competitive interest rates are common product features designed to lure customers away from existing branch accounts. However, despite the proliferation of retail Internet banks, there has been varied success in customer retention.

Insurance

Compared to on-line brokerage and on-line banking, development of the Internet in the insurance industry has been somewhat cautious. The effects of e-business are the subject of intense debate in the insurance industry, although actual translation into solutions is still in its infancy. In standardised personal lines insurance (e.g. motor, private liability and house hold contents), a recent Swiss Re survey predicts on-line channels to have gained a market share of 5-10% in the US, and 3-5% in Europe by 2005. In the area of standard products, where there is little need for advice, traditional brokers are facing considerable competition on account of falling information costs. In the cases of more complex products, particularly pension products, life assurance, health insurance and integrated risk management (IRM) products, competition has been less intense.

In Europe, three main companies dominate Internet insurance: the UK insurer Prudential, Skandia of Sweden (Skandia Banken) and AXA, a French insurer that has been very successful in the US with its DLJ Direct Financial Service.

A Forrester survey, (June 13 2000) has identified the rise of virtual insurance 'supermarkets' in response to consumer demand for comparison shopping for mortgages, insurance and funds. It is predicted that these will dominate the market by 2005.

A number of companies are now selling life assurance over the Internet directly to consumers. This is a sector which is sure to expand with the recent launch of the NetBank and Insurance.com co-branded web site being a good example. This site will provide customers with information and quotes on home, life, health and other insurance products.

Business-to-business ('B2B')

Business-to-business activities are most commonly seen in the following areas:

Securities

The bulk of activity in the wholesale securities market has been the creation of electronic networks for stock, currency and derivatives trading by existing investment banks and new start-up companies. Another securities development has been inter-business broking systems, providing full settlement facilities on-line.

The growth of such systems has been driven by the need to provide low cost automated execution capability. Such activities include the automated trading systems implemented by a number of the world's leading exchanges and the associated clearing and settlement facilities which support post trade processing. Increasingly, these are being challenged by Alternative Trading Systems (ATS) and Electronic Communication Networks (ECN) which provide execution capability outside the recognised exchanges.

For example, there are 39 new bond trading platforms in the United States, highlighting the popularity in this market of e-commerce. The secondary market has taken to screen-based trading through such order matching systems as Cantor Fitzgerald's e-Speed and Euro MTS. Goldman Sachs, Merrill Lynch and Morgan Stanley Dean Witter have recently (June 2000) announced plans to improve the way corporate and municipal bonds are traded, with the formation of BondBook, a company which will deliver an electronic system for bonds. A comparable venture is Bondclick, a price aggregation service for institutional investors to trade European government bonds. The mutual fund operators are not far behind and Europe's first mutual fund exchange, EMXco, will be launched shortly.

Many of these trading systems are now available on an international basis, particularly in Europe where the traditional national markets have been redefined in recent years. It is also interesting to note that the vast majority of these systems are regulated as broker-dealers but, in effect, fulfil the role of an exchange.

E-business in this type of environment differs from the Internet delivered services in that:

- They are restricted to institutional users rather than a wider retail base
- The users are sophisticated market participants
- The users have to satisfy, in many cases, strict membership criteria
- All parties, both users and service providers are subject to regulation
- Business processes are well established and robust, in most cases.

The growth of ATS is an example of the impact of the Internet on the financial services industry and the way in which the new technology has, to a very large extent, begun to disintermediate the market by bringing natural buyers and sellers together. The ATS provided by the broker dealers have reduced the role of and need for the exchanges and increased the availability and access to the markets. They are also an example of how fundamentals of regulation are being challenged. In the developing market environment, the previously clear-cut lines that differentiate the regulatory approach to markets themselves and service providers that use the markets are being blurred. The two regimes have different regulatory objectives and have different implications for the entities concerned.

The issues raised by the changing market infrastructure are many and are worthy of a 'thought paper' in their own right. US and European regulators have already consulted with the industry and the SEC, for example, has introduced specific rule requirements for ATS. In Europe, this matter is the subject of discussion within a specially formed Federation of European Securities Commissions (FESCO) committee. Therefore, whilst this paper looks at issues arising in the wholesale arena, it will not specifically address the issues arising from the changing market infrastructure and the role technology has played in this phenomenon. By their very nature therefore, the issues raised will predominate in the B2C arena.

Banking

On-line activity has proliferated in both corporate and investment banking. Corporate banking is the provision of deposits, loans, foreign exchange, payment services and settlement services to corporate customers. Investment banking includes underwriting for private equity offerings and Internet equity research. Other areas covered by wholesale banks are e-procurement and electronic banking payment processing. Two further market phenomena which will additionally impact securities and insurance are covered below.

Outsourcing

Financial institutions are increasingly outsourcing back and middle-office functions such as information and transaction processing activities. This is often due to the need to compress time to market, shortage of skilled programmers, cost reduction and economies of scale. Furthermore, it leaves time for financial institutions to focus strategically on core competencies and rely on other parties specialising in activities outside their expertise.

White labelling

The use of third party white labelled services is often sought for the same reasons as those seen in an outsourcing arrangement and is increasingly used to support a financial services portal strategy. The key here, from a regulatory perspective, is the relationship between the financial services provider and the white label services provider and the disclosure of that arrangement to the consumer. Often, both parties will be regulated in their own right, but it is vital that users of these services understand which is responsible for providing investor protection and under which regulatory regime.

Insurance

Commercial insurance has only a limited suitability for sale via the Internet. However, e-business facilitates better tailored products, shorter response times, greater flexibility in cover structures and better risk management reporting. A recent Swiss Re survey predicts cost cuts of \$11 billion in commercial insurance as a result of e-business. The same report also predicts growth in demand for liability, marine and credit risk insurance.

There are a number of emerging business models in the insurance B2B arena. Solutions providing support for policy administration and claims settlement are likely to dominate.

Other business models are:

- Insurance company web sites (homepages of individual insurers)
- Product portals (comprehensive standard web sites for financial and/or insurance products)
- Aggregators (Internet insurance brokers)
- On-line risk markets (large risks placed with trading partners)
- Point-of-sale portals (product marketing through various theme-based pages)
- Reverse auctions (auctions of insurance demand)

Forms of e-business media other than PC Internet access

This section briefly examines some of the other e-business media that will have a long-term impact on financial services businesses. As stated in the introduction, traditional Internet business is the core subject of this paper, while phenomena such as m-commerce will inevitably be the subject of further studies.

E-business is not only transacted via computers. Already, interactive banking is being provided through digital television (e.g. Open, Ondigital, Canal+). The customer can access different types of content,

depending on the offering of the particular service or content provider.

The mobile world is set to enter cyberspace. Wireless application protocol, or WAP, is a technology which links the Internet to wireless portable devices, such as mobile phones. This convergence is the beginning of a new way of doing business, 'mobile-commerce' (m-commerce). By 2004, there could be 700 million mobile commerce users worldwide.

This has led to interactive mobile phone banking, requiring customers to have their own WAP-enabled handset, allowing them to receive interactive content. They are then able to access Wireless Mark-up Language (WML)-based content from the on-line bank using WML browser software.

With the advent of WAP-enabled handsets, electronic money mediums are also being created. This will be an area where banks are able to use electronic payment networks to service customer needs over WAP or other forms of Internet access.

WAP-enabled handsets are not the only enabling technology for m-commerce access. In Japan, NTT DoCoMo, the country's leading cellular phone operator, has launched I-mode, a mobile phone service which offers continuous Internet access. This data communications service has already signed up several million customers and is still growing rapidly.

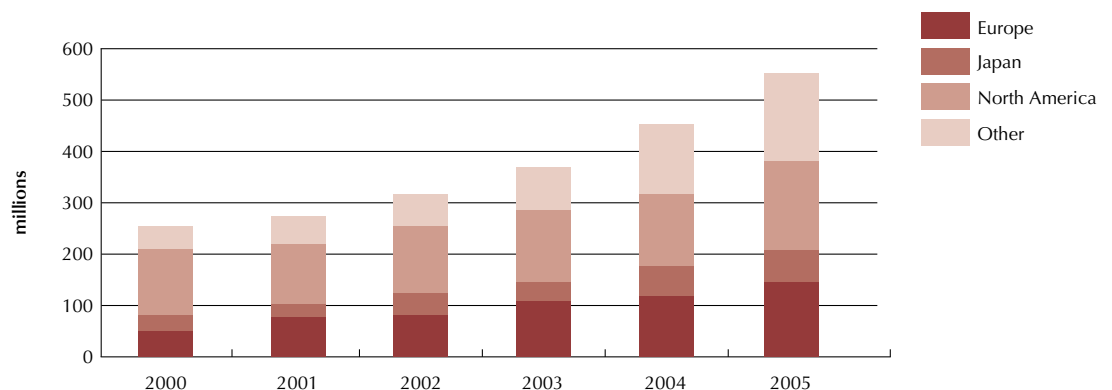
These media are set to grow rapidly in popularity, thus exponentially increasing the penetration and availability of e-business services. In Europe and Asia, the anticipated growth is such that WAP technology could eventually become the predominant form of accessing the Internet.

A report by Datamonitor on the future of banking in Europe predicts that by 2004, there will be 29.5 million customers using electronic means to bank. This is split into 6.1 million interactive TV users, 21 million Internet users and 14 million mobile users. Datamonitor also predict that in 2005, on-line channels will be the primary point of contact with banks for 35 million European consumers, compared with 4.5 million today.

Geographical analysis

Introduction

Figure 1.3 – Number of Internet users



Source: NUA Internet Surveys

At the beginning of this year around 250 million people were using the Internet around the globe.

This is projected to increase to 550 million by 2005 (NUA surveys).

Thus, the Internet is already a global phenomenon, and the number of international Internet users is set to continue to escalate exponentially. Currently, the United States is the leader among countries reporting e-business-related revenue, with some 80% of the global total, according to the OECD. E-business in Western Europe represents around 10% and Asia about 5% of world e-business trade.

However, countries that have lower rates of Internet penetration will see high growth rates over the next three years. Growth in Internet use will go hand-in-hand with growth in business to service Internet users needs. The financial services sector is at the forefront of that growth.

It is wrong to assume that the market size and the overall impact of the phenomenon are synonymous. The financial services sector has been affected disproportionately as the opportunities for electronic innovation are easier to identify earlier than in other industries.

United States and Canada

Currently, the United States is the global powerhouse of e-business usage. Today, in the United States, there are around 120 million users of the Internet. Approximately 35% of households use the Internet (NUA survey – May 2000). In April 2000, 8% of households were using on-line banking on the Internet (CSFI survey 'Internet Banking : A fragile flower'). Canada also has high Internet penetration.

For the year 2005, forecasts put the percentage of Americans with access to the Internet at more than 50%. By the year 2003, the amount of Internet commerce occurring outside the US is expected to exceed the amount that goes on inside the US. This demonstrates the current strength of the US position. Hence, developments in the US will have worldwide repercussions for Internet users. However, as the boom occurred first in the US, other continents can only catch up as they undergo their own electronic revolutions.

Europe

There are currently some 50 million Internet users (NUA survey) of the Internet in Europe, making it the second largest world market. Around 15% of Europeans surf the net (NUA survey – May 2000). The impact of the Euro may help accelerate the spread of e-business in Europe. Interbank transfers and transactions that use credit cards, debit cards, or electronic purses or cheques can be executed in Euros.

However, another phenomenon is anticipated in Europe that could eclipse customer PC Internet access, being the mobile phone or m-commerce. There are more mobile phone users in Europe than in the US, and although this is a nascent market, it could spark off a second e-commerce revolution.

Mobile penetration is particularly high in Scandinavia, which paves the way for a large growth in wireless banking. For example, SEB Group of Stockholm currently has 500,000 Internet banking customers. The head of strategy believes that they will have five million mobile-banking customers by 2004.

Asia-Pacific

There are currently around 33 million users (excluding Japan which has around 10 million users) – (Source: The Internet market in Asia Pacific – IDC survey). Over 25% of Australian households (1.7 million) have Internet access (ABS survey - Use of the Internet by Householders, Australia, November

1999 (Cat. No. 8147.0) released March 2000). Internet penetration in Japan and Australia is higher than the rest of the region.

Although Asia lags behind the US and Europe, there is clearly a vast population and huge potential for growth. The Japanese Internet commerce market, according to an IDC survey, will grow from \$1.5 billion to \$26 billion in 2002. China is another market with significant growth prospects.

Another important phenomenon in Asia is the rise in popularity of Internet access via mobile phones. With regard to m-commerce, Hong Kong is likely to be in the second wave globally (along with Singapore) behind Japan in terms of m-commerce developments and at least a year to 18 months ahead of the US and Europe.

Summary

This short analysis reveals how much is happening in the financial services marketplace and how this changes the way that financial services are being managed and delivered. There is no doubt we are in the middle of a revolution and that revolution is set to continue through the introduction of faster and more secure technology.

The concerns and risk factors

In the previous section, we looked at what is happening in the marketplace and how this changes the way that financial services are managed and delivered. In this section, we define what this changes in the regulatory arena and where the risks and threats, if any, are coming from. We also define the specific risk factors facing financial services e-businesses and take the debate a little further into specific sectorial challenges. But we start by considering why Internet delivered financial services need regulating at all.

Will the e-market of the future still need regulators?

With the ever increasing reach of the Internet into individuals and businesses lives, there is the possibility of getting much closer to the fabled perfect market so beloved of economists, whereby consumers are well-informed and a culture of self-regulation prevails.

'The Internet is potentially the Commission's greatest ally. It will help us accomplish the cornerstone of the Commission's approach to regulation – full and fair disclosure'

Commissioner Laura S. Unger
U.S. Securities & Exchange Commission

In the Internet world, information is much more freely available and is also provided more quickly. Access to this information seems likely to improve as users become more skilled and search engines improve.

It is possible, therefore, that consumers will have the right information readily available to them at all times, thus removing the need for active regulation. Businesses acting in an anti-competitive manner or breaching established market standards will be identified extremely quickly and customers will act on that information. The regulatory function is therefore replaced by the efficient market.

Such a scenario is, admittedly, unlikely. It is easy to argue, however, that there is very little in the new environment which suggests that the existing approach is inadequate and calls for radical changes in the approach to regulation, as detailed by the following:

- Sellers must still state what it is they are selling and why.
- Brokers' obligations to customers do not change as a result of on-line trading.
- Fraud is still fraud and those frauds perpetrated over the Internet are no different from the ones invented in the 1920s.

Additionally, conducting financial services business on-line provides many advantages to investors as:

- Emerging technologies, such as the Internet, have permitted smaller investors to gain access to information and analytical processes that previously were only available to professional investors.
- Costs are being driven down by competition, operating economies and disintermediation.
- The Internet will increasingly become a far more convenient way to conduct business.
- Banks, brokers, insurance providers and financial advisers will be open 24 hours a day, 7 days a week.

In the B2C arena, most Internet delivered financial services are provided by existing industry participants who are experienced in providing services within a regulated environment. As such, their e-commerce activities are merely a new medium for delivery and should not, in themselves, be cause for significant additional regulatory concern in their own right.

In the B2B arena, the emergence of technology-based marketplaces, where none have previously existed, is an opportunity for the industry to demonstrate its ability to self-regulate the integrity of the market infrastructure through the addition of liquidity, access, price discovery and settlement facilities to existing OTC markets.

Indeed, initial feedback from clients transacting in an on-line environment has indicated that the increased use of electronic applications has, in many cases, improved regulatory control. Where there are disputes over counterparties or transactions, it is now easier to refer back to electronic records. Furthermore, employees can be encouraged to fill in electronic procedure sheets before the system allows a certain task to be completed. This may reduce the chances of a regulatory breach.

As the Internet develops, it is a given that there will be a tension between avoiding over-regulation (so that it will not collapse under the strain of sheer demand from users) and ensuring that consumers will benefit from a competitive marketplace. As ever, finding the balance is the regulators' challenge, but the potential regulatory benefits that the technology can deliver should not be lost on the regulators or the regulated.

Why does it need regulation?

So, it is good news for the consumer and great news for the markets – why, therefore, do we believe that the Internet is worthy of particular regulatory scrutiny? The answer is that B2C regulation is, fundamentally, about providing consumer protection and regulators should, therefore, be concerned about the effects of on-line delivery in the market as the Internet, increasingly, puts investors at financial risk through:

... regulators should, therefore, be concerned about the effects of Internet delivery in the market as the Internet, increasingly, puts investors at financial risk ...

- Fraud
- Chat-room share ramping
- Mis-selling
- Unauthorised service providers
- Lack of privacy of information
- Lack of reliability of service through poor accessibility performance (business continuity planning)
- The immediacy of the medium

In terms of the market infrastructure, the potential risks associated with increasing IT dependency mean that new challenges have arisen around the regulation of the infrastructure itself.

Fundamentally, therefore, financial services providers over the Internet need regulating for exactly the same reasons as financial services delivered via any other medium. These are:

- A stable financial system provides a favourable environment for efficient resource allocation and, therefore, promotes economic growth. Time has shown that, left to themselves, financial systems are prone to bouts of instability and contagion. In an increasingly electronic environment, it could be argued that the risks of contagion arising from systems failure are substantially increased.
- The second prime justification for financial regulation arises from the nature of the market for retail financial services. It is a market characterised by asymmetric information, which makes it difficult for buyers to assess the risks and returns of the transactions they undertake. Without regulation to give consumers some independent assurance about the terms on which contracts are offered, the safety of the assets which underpin them, and the quality of advice and information received, saving and investment is discouraged, again with damaging economic consequences. The Internet encourages new players and new products to the market and opens up the range of products available to those sold on a cross-border basis as well, thereby exacerbating the asymmetric characteristics of the market.

The advent of electronic delivery has raised new challenges and brought into question existing compliance processes as well, including the following:

Regulatory challenges

- Electronic delivery brings with it a lack of transparency. On the Internet, any firm can appear to be enormous, research can sound credible, individuals can appear qualified, all without any real foundation.
- The industry will, increasingly, rely on IT capability which brings with it systemic risk and investor confidence responsibilities.
- The Internet opens up new opportunities for financial crime including share ramping, the marketing of fraudulent services and money laundering.

Process challenges

- Jurisdictional boundaries are no longer relevant in cyberspace.
- Paper-based communication and record keeping requirements are outdated.
- Compliance-monitoring procedures are failing to keep pace with the innovation in delivery.

The way forward

One of the great strengths of the Internet is that it is unregulated and therefore able to evolve quickly and naturally. We certainly see no valid argument for advocating regulation of the medium itself.

There are, without doubt, new regulatory challenges that come with the medium. This is a governance issue in respect of which the industry should take responsibility for developing good market practice. This will in effect produce an environment of self-regulation that will address many of the issues that have arisen. The role of the regulators is to ratify and enforce such practices and, only in the case of some extreme issues, bring an independent perspective to the party where intense competition is restricting the development of good market practice.

Where is the threat coming from?

We have already concluded that on-line financial services require regulation and have suggested some of the potential threats that have led to that conclusion.

However, threats come in a number of forms. The Internet also offers great opportunities and there is a further risk that over zealous or outdated regulation of Internet-delivered financial services may undermine these opportunities and, as such, offer a threat in themselves.

In summarising the threats, therefore, we have considered them from a consumer, an industry and a service provider perspective, as follows:

Threats to the consumer

- Unregulated services marketed without the 'backing' of capital adequacy supervision, investor protection and conduct of business rule requirements
- The information and expectation gaps which exists between customer expectations and reality when buying on-line
- Denial of service through systems downtime, i.e. system unavailability preventing consumers from accessing markets and potentially suffering financial loss
- Poor investment decisions provoked by the immediacy of buying on-line
- Fraud, security and lack of privacy of information

Threats to the industry

- IT systems dependency which creates systemic risk and has the potential, through a high profile 'failure', to undermine investor confidence.
- An inexperienced marketplace where new entrants capture large market share without the experience of having operated within a regulated environment and backed only by minimum regulatory capital.
- The inability of outdated rules, supervision and monitoring techniques, both within the regulator and the regulated, to keep pace with the increased speed of delivery of financial services.
- Uncertainty regarding the application of pre-electronic rules in an on-line environment, i.e. suitability requirements.

Threats to the financial service providers

- Lack of e-business management expertise
- Jurisdictional constraints
- Hacking, theft and other forms of systems abuse
- Internal and external fraud
- Unsuccessful transition to a paperless society
- Privacy constraints

We shall now look at the main concerns and threats in greater detail. These issues impact, to a varying degree, on the key industry sectors. Table 2.1 illustrates where the differences lie.

Jurisdictional constraints

The Internet is global, by its very nature, yet on-line financial services continue to be regulated on a jurisdictional basis. Global financial services businesses are increasingly concerned by the lack of consistency in the different regulatory frameworks around the world. The absence of compatibility and consistency between approaches at a global level is already seen as a barrier to innovative use of the Internet in financial services.

'In terms of the technology itself, that means that firms have realistic business plans, that their computer capacity matches these plans, that the capacity can be readily increased, that there are effective security procedures in place both as regards unauthorised internal access and external hacking, that data integrity is preserved during system crashes, including data being processed at the time of the crash, that proper record keeping arrangements exist, and so on.'

**UK Financial Services Authority
November 1999**

IT Competence

If the Internet is to accommodate the rapid growth predicted, and provide a sound, long-term foundation for e-business, web-sites must not only be available at all times, but also be highly reliable. New technologies create new risks and management must understand the various risk issues that are core to those technologies and review risk management policies and procedures.

Accessibility to services is absolutely vital in all areas of the financial arena. Systems downtime is one of the biggest risks for consumers when transacting with an on-line provider. Without effective business continuity planning both consumers and the industry face the risk of financial loss

There is no doubt that this is a key issue for the industry to address on an ongoing basis. There have been too many examples of systems failures in the industry, many of which could

Table 2.1 - Issues facing different industry sectors

Key regulatory risks	Banking	Securities	Insurance
Consumer			
1. Expectation gap	○	●	●
2. Denial of service (systems failure)	●	●	○
3. Unauthorised service providers	●	●	●
4. Suitability	○	●	●
5. Privacy	●	●	●
6. Cybercrime	●	●	●
7. Poorly informed investment decisions	○	●	●
Industry			
1. IT systems dependency	●	●	●
2. New entrants	●	●	●
3. Out-dated rules, supervision and monitoring techniques	●	●	●
4. Uncertainty regarding the application of pre-electronic rules in an on-line environment	○	●	●
Financial service provider			
1. Lack of e-business management expertise	●	●	●
2. Jurisdictional constraints	●	●	●
3. Successful transition to a paperless society	●	●	●
4. Privacy constraints	●	●	●
5. Cybercrime	●	●	●
KEY:	● High impact/probability	● Medium impact/probability	○ Low impact/probability

have been avoided with the appropriate IT planning and testing. Please refer to Appendix 1 – ‘To be in (e-) business tomorrow, what should financial services companies be doing today?’ – for a list of recommended actions for e-businesses.

Lack of e-business management expertise

E-business is relatively new in the financial services arena and, as a result, there can be a lack of understanding among senior management about its potential and implications. People with technological, but not financial services, skills can end up driving the initiatives. E-initiatives can spring up in an incoherent and piecemeal manner in firms. They can be expensive and can fail to recoup their cost. Furthermore, they are often positioned as loss leaders (to capture market share), but may not attract the types of customers that banks, brokers or insurance companies want or expect and may have unexpected implications on existing business lines.

Firms should respond to these risks by having a clear strategy driven from the top and should ensure that

this strategy takes account of the effects of e-business, wherever relevant. Such a strategy should be clearly disseminated across the business, and supported by a well-defined business plan with an effective means of monitoring performance against it.

Cybercrime

While appreciation and understanding of the Internet may be a challenge to many of us, the mischievous and malicious have found it a new and useful source of fun. The following statistics are taken from two independent industry surveys :

- On average, every site newly installed on the Web will be accessed within 28 seconds and attacked within 5 hours.
- 60% of hackers said the opportunities for accessing systems are increasing, aided by the growth of the Internet.
- 75% of organisations surveyed reported financial losses due to security breaches ranging from financial fraud to theft of proprietary information to laptop computer theft.
- 60% of networks are penetrated over 30 times a year.

Table 2.2 gives an overview of the nature of cybercrime. However, as stated above, these are not new felonies, rather variations on existing themes. As such, the regulatory and legal authorities are in a position to adapt policies and procedures rather than starting from scratch.

Cybercrime is certainly an issue for the industry and the following are just two examples of actual criminal activity on-line:

Table 2.2

Crime	Paper-based	Cybercrime
Unauthorised access	Breaking and entering	<ul style="list-style-type: none"> • Password snooping • Computer misuse
Vandalism	<ul style="list-style-type: none"> • Physical graffiti • Billboards • Arson 	<ul style="list-style-type: none"> • Web-site hacks • Viruses
Obstruction	Obstruction	Denial of service attacks
Theft (money)	Theft of cash	Electronic funds transfer
Theft (assets)	Theft of physical property	Software piracy
Theft of intellectual property	Infringing copyright	Copying digital images and files
Impersonation	Forgery of signatures	e-mail spoofing
Misuse of company property	Abuse of mail-room facilities	Excessive web surfing

- In 1997, the US Federal Trade Commission began litigation against a company called 'Fortuna Alliance' which had an Internet site. This company offered investors a return of \$5,000 per month for an investment of \$250. It might be thought that no one would be foolish enough to invest in such an improbable scheme but in fact investors lost about \$6 million before the FTC blocked access to the site.
- In August 1997, the European Union Bank, which traded over the Internet, collapsed. It was registered in Antigua and had been founded by two Russians in 1994. The site claimed that it offered a US\$1 million certificate of deposit that paid interest of 9.91%. It had attracted unfavourable comment by the Bank of England some time before it collapsed.

There is still insufficient reliable data to measure just how big an issue it actually is. However, it is definitely an issue in respect of which all users of the Internet should act diligently and every effort must be made, when employing new technology, to build firewalls around the integrity of confidential information and the financial system as a whole.

Cybercrime is also evident in other areas such as fraud and money laundering. The potential for anonymity within the medium, means that the Internet is an attractive home for money launderers and fraudsters (for example, share ramping). The need for reliable means of identifying third parties is, therefore, vital in addressing these issues and ensuring the ongoing success of e-commerce

Unregulated service providers

The unstructured environment offered by the Internet and similar media represents a whole new set of regulatory problems.

The immediate and global nature of the Internet means that services can be provided:

- From unregulated jurisdictions
- On a largely anonymous basis
- Directly to the homes and workplaces of potential users

This makes detection of unregulated financial services almost impossible for domestic regulators.

Direct business-to-consumer electronic commerce will not reach its full potential until consumers are assured that the on-line environment is a safe and predictable place for them to do business. In the 'real world', domestic markets offer investors assurances that their transactions are covered by national legal and private sector consumer protection.

However, in the global electronic marketplace, such protection cannot be taken for granted. The lack of face-to-face contact between businesses and consumers increases the need for a trustworthy electronic marketplace.

New entrants

Whilst every effort is made to ensure that established market participants are properly regulated, it is the new entrants who typically pose the greatest risk. Potentially, this market segment could create a disproportionate risk to consumers, and the industry, of financial loss through failure.

... greater risks and regulatory challenges, as the number of new entrants increases and the relative experience in the industry decreases ...

Technology is breaking down barriers to entry into the industry and challenging traditional methods of conducting investment business. New participants in the industry, such as First-e in on-line banking, are good examples of start-up entities which have already appeared in Europe. In the US, where the Internet market is more advanced, there are now large financial services businesses built purely on the back of on-line activity; on-line

brokerages are good examples.

This trend is likely to continue and bring greater risks and regulatory challenges, as the number of new entrants increases and the relative experience in the industry decreases. Additionally, the delivery of financial services will become evermore reliant on interactive IT systems, and the growth of ATS facilitating wholesale broking activities is a good example of this. Reliance on systems increases systemic risk and the challenge to the industry is to get the systems design and implementation right so that this does not

necessitate further regulatory intervention in this area. The challenge to regulators is to keep pace with innovation and change and retain 'control' in a rapidly changing marketplace.

There is increasing evidence of on-line financial services providers expanding their product portfolio and thereby taking advantage of the ease of access to their client base through Internet technology. This is fuelled by the portal concept and is likely to further challenge the 'process' of regulation where regulated firms, other than the largest global businesses, are conveniently packaged up into, for example, deposit takers, brokers, fund managers, retail service providers, etc.

There is also evidence that the speed of introduction of new products often means that the necessary management oversight, technology, controls and compliance arrangements lag behind innovation.

Privacy

Due to the global nature of the Internet, information is transmitted across several borders and jurisdictions. If companies on the Internet are to gain the confidence of customers and, indeed, if governments wish to see the success of this phenomenon, protection of users, in particular with regard to privacy, confidentiality and anonymity should be assured.

Specific risks arising from privacy issues include:

- On-line privacy statements are not accurate with respect to practices.
- Inconsistencies between on-line and off-line practices and policies: customers may be led to believe that the privacy practices that they have been accustomed to in the 'off-line' world are the same in the on-line world.
- Third party collection of 'clickstream' data tracking visitor's site interests and navigation habits could reveal sensitive information (e.g. visits to HIV/AIDS related interest groups, financial planners, rate quote toolkits, etc).
- Failure to maintain adequate security of personal data accessible from site. The lack of security of data may lead to access of customer data by third parties for improper social or commercial use.
- Weak links in chain of trust with third parties linked from site.
- Lack of control over agent/agency sites, especially independent agents.

Further threats to the privacy of information arise from the increasing threat of Internet vandalism. Evidence of this is seen in the UK where the government is proposing the 'Regulation of Investigatory Powers Bill' in order to prevent the effects of viruses such as the 'I Love You Bug'. This legislation would give the police and other officials the power to intercept e-mails and mobile phone communications.

Suitability

Suitability of information provided to users in the on-line environment is at the forefront of concern for the regulators, particularly in the United States. The concern stems from the fact that data profiling of customers, based on on-line behaviour, is being used by on-line brokers to make recommendations that may not be 'suitable' to the customer's financial situation, objectives and needs. In an environment of increasing technological capability, brokers can customise investment information and investment services for on-line investors and this is complicating the matter of determining what is a recommendation and what is not.

This is particularly an issue where a client is an 'execution only' customer who, in an 'off-line' world, would not have been entitled to any suitability 'protection' from the broker. Advertising has always had to be fair and not misleading but the distinction between mere advertising and actual advice is becoming increasingly blurred and, with it, the conduct of business obligations of the broker.

Information gap

Making investment decisions through on-line brokerages has been revolutionised, and is often perceived as easy, cheap and instant; e.g. on-line brokers advertise that a trade is no more than a 'click'. An information gap exists between customer expectations and reality when buying on-line. Often, the investor expects direct and immediate trade executions while on-line brokers expect to provide a faster routing mechanism to the marketplace. A 'click' merely represents a request for a trade, and the customer cannot execute a trade without reliance on a broker-dealer.

Clicking the mouse may be easy but making sound investment decisions is not. Aggressive advertising has fuelled the misconception of easy wealth and the risk of being left behind in the new on-line era. Therefore, financial institutions should ensure they are providing information that is not misleading.

Furthermore, in each e-commerce transaction, there is always a third party involved; e.g. the Internet Service Provider. Therefore, the risk of computer system breakdown is difficult to eliminate, even if the financial institutions and the users of those services take thorough preventive measures.

It is highly possible that service customers are taking part in transactions without any conscious awareness of these third parties. For example, if a transaction has been delayed or interrupted but the delay or interruption cannot be directly attributed to the financial provider, it is possible that disputes between the service customer and provider can arise due to biased impressions on the part of the customer. Hence, the financial institution should ensure that customers are aware of the existence of such risks, and possibly provide them with alternate contact methods in situations of system outage.

Successful transition to a paperless society

Businesses are rapidly moving towards a paperless world as a cheaper and more efficient means of conducting business applications. As companies at earlier stages of the value chain convert their processes to an electronic medium, companies further along the chain will also have to convert their applications.

The primary concern is that the transition to a paperless society may not be successful, thus failing to recognise and address the additional risks of e-commerce to the business and its customers.

A number of new risks do arise and it is vital that these are managed effectively. Examples include:

- The lack of personal contact is challenging for institutions to verify whether customers are bona fide. This is an important element in making sound credit decisions.
- As the Internet spans many jurisdictions, business will increasingly be conducted with foreign investors which will create exposures denominated in a foreign currency or funded by borrowings in another currency.
- A 'bricks and mortar' financial services company's reputation can be damaged by Internet services that are poorly executed or otherwise alienate the customers and the public.
- A high level of transaction risk may exist with Internet products, particularly along lines of business that are not adequately planned, implemented and monitored.
- Most Internet customers will continue to use other financial services delivery channels. Financial services companies will need to make sure that their disclosures are synchronised with other delivery channels to ensure the delivery of consistent and accurate messages and services to customers.
- Failure to link the technology employed in providing products and services beyond the trade area to the strategic planning process may increase the strategic risk.

Moving to a paperless society requires thought, planning and capability. Failure to innovate new products while maintaining the 'luxuries' of an on-line world may result in reducing the value added to the business and to society as a whole.

Summary

There are many risks relating to buying and selling over the Internet. However, it is not the role of regulation to eliminate financial risk wherever it arises. Risk is an intrinsic feature of financial products, and it is the role of the financial markets to manage, allocate and price risk. The regulatory mandate is to find the balance between protecting consumers and letting the markets function without excessive interference.

For many and varied reasons, electronically delivered financial services certainly require regulation. They require regulation for the very same reasons as more traditionally delivered financial services. However, they also bring with them new risks, challenges and, of course, potential rewards.

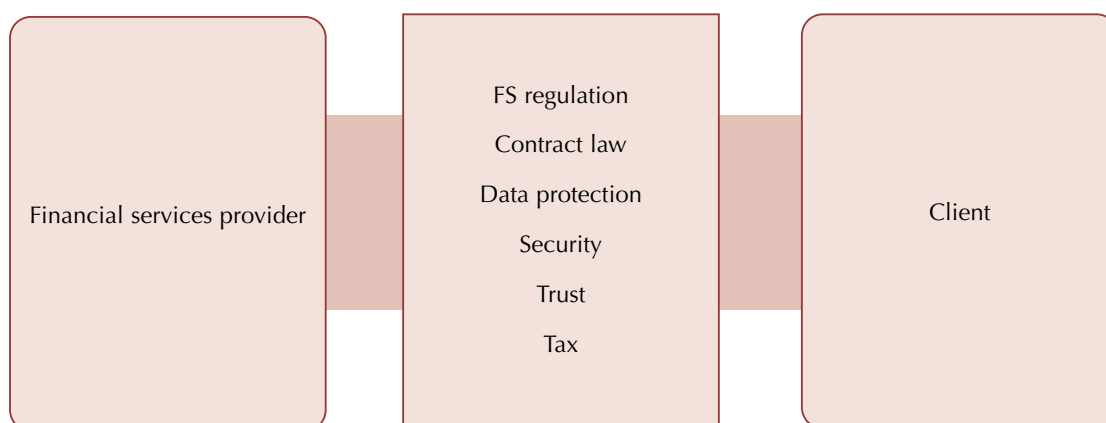
This means that regulators must address the new risk factors and face up to challenges to existing regulatory practices. For its part, the industry must use the technology in a responsible manner and ensure prudent management techniques are applied equally in an e-environment. Only then will the true benefits of the Internet be delivered to investors.

How have the regulators addressed the challenge?

In the previous section we concluded that the changing characteristics of the financial services market are opening up a raft of new regulatory issues and that the development of the Internet is raising particular challenges for investor protection. We now move on to explore how regulators have responded to the challenge, differentiating, where appropriate, between individual markets at varying levels of maturity.

When conducting a transaction on-line, a large number of issues are raised which are characterised by a mixture of uncertainty, complexity and originality. This report focuses on the questions surrounding financial services regulation, although it does, by necessity, refer to some of the other issues detailed in figure 3.1.

Figure 3.1



The current environment

Regulators are already expected to cope with a wide range of responsibilities against a background of limited human resources. Effective regulation requires the development of a close partnership between the regulators and the regulated and the financial services industry now has the opportunity to set the framework for future on-line financial services regulation. A telling example of this can be found in the changing market infrastructure. The ownership of the new infrastructure will move away from long-established, well-capitalised and closely regulated businesses (i.e. the major trading houses) toward new entrants with a limited track record and even less capital. However, many of the new entrants are supported by a number of the major trading houses, often as part of a consortium. As sophisticated market participants, the institutions using the new automated trading systems will need to be satisfied that they are suitably robust and resilient before they agree to transfer any significant volume to them. While the ownership of the infrastructure may change, therefore, the same market participants retain an underlying interest in safeguarding its health, and the willingness and ability to self-regulate remains paramount.

The regulatory response to date

The response can be summarised by the following:

- Guidance releases
- Policy papers
- Speeches

These have covered the need to apply the same prudent management techniques to e-businesses as more traditional enterprises and have identified the additional risks that regulators believe arise in an on-line environment.

Greater international co-operation has begun to address jurisdictional problems, though development in this area is embryonic.

Finally, legislators are supporting the regulatory effort where possible with the introduction of e-friendly statutes and the updating of legislation such as the recognition of digital signatures.

We start by outlining progress in two of the key areas for e-regulation:

- The international response to cross-border and jurisdictional anomalies
- The response at a national level to IT capability issues

We then examine, more specifically, the responses from national regulatory authorities, where they exist, regarding financial services Internet regulation.

The jurisdictional challenge

Regulators currently have to deal with developments in their own domestic markets and their responses to date have largely been dictated by the maturity of e-commerce within their jurisdiction. However, regulators are mindful of the cross-border challenges facing the financial services industry and there is considerable evidence of greater global co-operation among regulators through international organisations aimed at addressing these issues. Examples include:

- Through the International Organisation of Securities Commissions (IOSCO), regulators have largely agreed on the 'targeted at' principle which, subject to certain technical definitions, means that web sites will only be subject to regulatory requirements in the jurisdiction(s) to which they are directly targeted.
- International Internet Surf Day on 28 March 2000, launched by the IOSCO Technical Committee, was aimed at increasing investor protection and market confidence. Twenty-one securities and futures regulators from 18 countries co-ordinated their efforts to identify securities and futures fraud on the Internet.
- The theme for the IOSCO annual conference held in Sydney in May 2000 was 'Global Markets – Global Regulation'. IOSCO's Internet Task Force is currently developing further guidance on regulation and surveillance of Internet securities activity. Issues being discussed by the Task Force include disclosure, investor protection, information sharing, web site contents, new Internet developments and the practical implications of jurisdictional control, along with surveillance and enforcement.
- The Electronic Banking Sub-Committee of the Basel Committee on Banking Supervision is currently examining supervisory issues for Internet banking.
- IOSCO, the Basel Committee and the International Association of Insurance Supervisors (IAIS) came together in the 1999 Joint Forum. Documents released by the Joint Forum outline

principles for banking, securities and insurance supervisors aimed at ensuring, through the regulatory and supervisory process, the prudent management and control of 1) risk concentrations and 2) intra-group transactions and exposures.

- The International Insurance Regulatory Issues Work Project of the IAIS is drafting the standards of supervision for electronic insurance transactions.
- The Organisation for Economic Co-operation and Development (OECD) Forum 2000 was held in Paris in June. The overall focus was 'Partnerships in the New Economy' and the key themes included tackling issues surrounding the e-commerce environment.
- The Forum of European Securities Commission (FESCO) initiated an Expert Group for Alternative Trading Systems in December 1999 to study the risks and benefits associated with such facilities.
- In October 1998, the OECD and the Government of Canada jointly organised a Ministerial Conference on e-commerce. As a result, three action oriented documents were tabled: the OECD Action Plan for Electronic Commerce, the Report on International and Regional Bodies: Activities and Initiatives in Electronic Commerce and the Global Action Plan for Electronic Commerce prepared by Business with Recommendations for Governments, outlining for the first time who is doing what to solve these various problems. Commitments coming out of the Conference include consumer policy issues, social and economic impacts, privacy and the protection of personal information, authentication mechanisms and standards, and access to information infrastructure.
- FESCO has issued a consultative paper on standards for regulated markets as it believes additional European guidelines are needed to take account of developments in technology. The paper highlighted that firms providing clients with an 'electronic link' should 'have proper safeguards in place'.
- FESCOPROL was created in January 1999 following the launch of the FESCO Multilateral Memorandum of Understanding on the Exchange of Information and Surveillance of Securities Activities. The protocol is in response to the increasing internationalism of the European financial markets. It aims to create a pan-European regulatory framework to provide possible mutual assistance between members aimed at enhancing market surveillance and effective enforcement against financial abuse.
- There are a series of memoranda of understandings in place that pre-date the electronic age but support, nonetheless, cross-border co-operation in an increasingly global marketplace. New agreements are also being forged.

Supervision in today's global environment can only ever be effective if it has an international dimension. Naturally, regulators have long had to deal with the problems of monitoring multinational business. They have established mechanisms for cross-border supervision, including accords covering home/host responsibilities (especially within the EU) and bilateral agreements for information sharing and general standards by which they expect all banks, including those in offshore territories, to abide.

Inevitably, however, the nature of e-business raises particular challenges in how to apply the general principles outlined above. It makes it even more important to develop a cohesive international approach to regulation – not only in the field of prudential regulation where Basel has made considerable progress, but also in the related area of consumer protection.

Further progress, in banking for instance, is likely to come from such bodies as the Basel Committee E-Banking Group, which believes that the eventual accord "should provide the international supervisory community with a broad set of advisory guidance with respect to electronic banking," thereby providing a basis for domestic regulation and supporting consumer and industry education. Globally, such guidance would enhance international co-operation and act as a foundation for a coherent approach to supervising e-banking. It could thus pave the way for the rapid expansion of international e-banking by creating consumer confidence in sound banks based in different, possibly less satisfactory, regimes and, in

addition, might dissuade host supervisors from imposing any extra, potentially draconian, regulation on such banks.

However, looking at international co-operation as a whole, we believe that there is a disproportionate emphasis on supervision and enforcement in cyberspace compared to the economic demands of facilitating cross-border activity. E-commerce highlights existing differences between legal, contractual and judicial systems. The national variations in private and contractual law, along with the differences in cultural preference, mean that the determination of the applicable law to an electronic consumer contract and the rules to determine liability are of particular relevance. Many electronic transactions cut across different jurisdictions, thus giving rise to the urgent need to address these regulatory anomalies.

Although such issues are of concern for all on-line service providers, they are of particular importance for finance. Financial services providers need to know whether they have to comply with the regulatory provisions in the jurisdictions in which they offer on-line services and how these apply in practice. Until legislation does come into force on a global basis, those contemplating e-business projects will need to evaluate their operations in light of today's inconsistent legal and regulatory structure. Generally, this requires an ad hoc approach, which can only be at odds with the philosophy and potential of the Internet.

The IT challenge

The regulatory response to the IT challenge has been mixed, with regulators outside the USA showing little appetite for setting specific IT standards, though individual offenders can expect a firm hand. In the US, regulators have addressed some issues specifically and, through the FFIEC handbook released by the OCC, have produced an inter-agency guide to assist those responsible for overseeing financial institutions and independent service bureaux. The Handbook covers the regulatory policies of FFIEC member agencies for use in examination of information systems and acts as a:

- Tool for better supervision and examination guidance
- Training aid for new IS examiners
- Reference source for the industry under supervision
- More comprehensive technical reference source

Elsewhere, national regulators are beginning to demonstrate a greater interest in the regulated communities' IT capability, focusing on service providers, intermediaries and the exchanges themselves. The UK Financial Services Authority (FSA), for instance, has brought this issue to the fore by setting demonstrably higher competency standards for IT dependent firms – especially new entrants into the industry. The checks include detailed questioning of policies and procedures, review of systems documentation and on-site visits. The FSA now routinely assesses the IT capability of new entrants, using auditors' reports to support this evaluation, where appropriate.

In Japan, the Centre for Financial Industry Information Systems has devised an industry-wide autonomous standard known as the 'Proposed Standards for Computer System Safety Measures in the Finance Industry'. This sets out common guidelines for safety measures to be employed for investigations or the testing of new systems. However, further refinements will be required to keep pace with technological developments.

We now summarise and compare some of the responses from regulators in key geographical locations. This is not intended to be exhaustive, but rather a summary of some of the key responses, citing certain national regulatory authorities for illustrative purposes.

Banking

America

According to William J. McDonough, President of the Federal Reserve Bank of New York, “there are three elements of a modern supervision framework – effective bank level management, market discipline and official supervision”.

The OCC believes that “government must refrain from unnecessarily interfering with market forces propelling innovation forward” (Testimony of James D. Kamihachi, Senior Deputy Comptroller for Economic and Policy Analysis, March 1999). As a result, the OCC has tried to focus the attention of bank regulators on areas where markets “may fail to address the concerns raised by emerging retail banking and payments technologies.”

Recent examples include the ‘Comptrollers Handbook on Internet Banking’, published in October 1999, which explains the risks associated with Internet banking and best practices for their avoidance. Various bulletins offer further guidance on particular aspects of market and technological development, such as the OCC Bulletin 99-20 covering Certification Authority Systems and Examiners and OCC Bulletin 98-38 on personal banking.

The FFIEC has also issued some guidance and information outlining federal laws and regulations on consumer protection and how they apply to electronic financial services operations. The FFIEC’s ‘Guidance on Electronic Financial Services and Consumer Compliance’ looks at how current legislation covering deposit services and loan leasing services is applicable to applications on the Internet.

The FDIC has issued guidance on ‘Safety and Soundness Examination Procedures’. Consistent with the federal authorities’ bulletins, this sets out potential risks and summarises the mitigating controls.

Europe

The response has tended to focus on ensuring that banks continue to be managed prudently in an e-environment, through guidance and speeches highlighting the risks inherent in on-line banking. The main concerns include:

- The impact of e-banking on traditional services.
- Strategic risk – do senior management understand the potential and implications of e-commerce?
- Business risk – as e-banking is a relatively new innovation, little is known about how the characteristics of e-customers might differ from their traditional counterparts.
- Operational risk – banks face three main types of operational risk:
 - Accurate volume forecasts have proved difficult which may create systems scalability problems.
 - Banks may have difficulties in obtaining adequate management information to monitor their e-service.
 - Outsourcing key functions can create material risks by potentially reducing a bank’s control.
- Security is a key priority both inside and outside the banking industry.
- Reputational risk – banks must ensure that their crisis management, particularly PR, processes are able to cope with Internet-related incidents.

The level of response differs between the member states due, largely, to the different maturities of the Internet banking sectors in those states. The Scandinavian countries, in particular, have highly developed Internet banking sectors; the UK authorities have also been active in this area as the UK Internet banking sector develops.

Asia-Pacific

The Australian Prudential Regulation Authority (APRA), which oversees banks, insurance companies and superannuation funds, credit unions, building societies and friendly societies, is currently examining the impact of e-commerce on financial services. APRA is keen not to stand in the way of innovation in this developing area through the application of unnecessary rules and regulations. APRA's Policy Program, launched in March 2000, includes a new consultation document aimed at stimulating debate on this increasingly important activity.

The regulatory framework for banking in Hong Kong is divided into two main parts – e-money in the form of stored value cards and electronic banking channels. The HKMA has issued a number of general circulars on e-banking, focusing in particular on the need for security. Authorised institutions wishing to move into e-banking would need to:

- Demonstrate how they would restrict access to the system and its databases to sanctioned users
- Authenticate the identity and authority of the parties concerned to ensure the enforceability of transactions
- Maintain the confidentiality of information while it is in transit through the network
- Ensure that the data has not been modified either accidentally or fraudulently

The HKMA insists that such Internet security arrangements should provide an adequate audit trail. Authorised institutions must also draw up contingency plans to maintain the availability of services, particularly in the provision of time-sensitive information and processing value-bearing transactions. However, the HKMA accepts that there can be no absolute security in cyberspace and expects that the level of cover should be 'fit for purpose'. Accordingly, it stipulates that risk management systems and internal controls should be regularly reviewed and evaluated.

The HKMA recently issued its 'Guidelines on the Authorisation of Virtual Banks'. The basis of this document is the insistence that e-banks must have substance rather than simply being a concept. Virtual banks, therefore, need to have a sensible and coherent business plan which addresses the various types of risk they face and which strikes an appropriate balance between acquisition of market share and earning a reasonable rate of return. Such thinking is largely common across all banking and prudential regulators.

The HKMA is now considering the need for more specific recommendations covering information security in Internet banking. We understand that these recommendations, which are under review, will focus on security and operational resilience requirements. The HKMA also intends to amend the Banking Ordinance for advertisements placed on the Internet for deposits. In particular, this will clarify the extent to which telecommunication and Internet service providers should be subject to these rules. In a parallel move, the HKMA is looking at how to strengthen its supervisory powers in relation to the offer of banking products and services on-line.

In April 2000, the Federation of Bankers associations of Japan drew up a report entitled 'Considerations with Respect to Internet Banking'. Priorities include:

- The establishment of in-house problem management infrastructure
- Security assurance protocols
- Response measures for data input errors (e.g. display structure improvements, etc)
- Clarification of items for which exemption from liability is allowed
- Display of information on precautionary measures
- Prevention of illegal transactions
- Measures for system breakdowns
- Establishment of consultation facilities
- Preservation of transaction records, etc

Securities

America

In common with other such bodies in the US, the SEC has not adopted an “entirely new regulatory approach” (Speech by Commissioner Laura S. Ungar at the conference on ‘Integrating Technological Advances for On-line Brokerages’, New York, September 1999). Instead, it is concentrating on the following criteria to enable it to fulfil its primary mission of protecting the investor:

- **Enforcement programme**

The SEC’s Internet enforcement programme is centralised in the Office of Internet Enforcement (OIE). The OIE oversees the SEC’s ‘Cyber force’ which brings together 250 lawyers, accountants and other staff located throughout the US. This acts as an ‘Internet police force’, surfing the network for any potential securities frauds. The enforcement programme has come across three traditional types of Internet fraud: market manipulation, illegal touting and frauds arising from public and private securities offerings. As a result of this programme, the SEC has brought several cases to court, which it believes will act as an active deterrent to future fraudulent activity. Notable cases include NEI Webworld, FastTrades.com and Dynamic Trader.
- **Investor education programme**

The SEC has made investor education a key part of the fight against securities fraud. It believes that an investor who knows what questions to ask and what kind of illegal practices are prevalent can act as a good “defence and offence” to Internet fraud (Speech by Laura S. Ungar at IOSCO Annual Conference, Sydney, May 2000). The SEC has launched a variety of initiatives and has recently set up an investor education page on its web site.
- **Corporate disclosure**

High on the list of the SEC’s priorities is the issue of suitability. This has been addressed extensively in a separate study by Commissioner Ungar entitled ‘On-line Brokerage: Keeping Apace of Cyber-space’. Published in 1999, the report focused on these key areas:

 - Suitability
 - Best execution
 - Market data
 - Systems capacity
 - Investor education
 - On-line discussion forums
 - Privacy
 - Portals

The study concluded that “although it may still be premature for extensive rulemaking in this area, this report highlights for the Commission certain key issues facing investors and the industry and recommends how the commission can resolve some of these issues.” The National Association of Securities Dealers (NASD) has advised its members that transactions that are not recommended do not give rise to a suitability obligation. The SEC’s counter argument is that in the on-line world it can be difficult to determine what is a recommendation and what is not. In order to help clarify this issue, Commissioner Ungar’s study poses seven hypothetical scenarios and shows what is likely to be subject to a suitability review and what is not.

There has been similar progress at state level, notably a report issued by the New York State Attorney General, Eliot Spitzer, entitled ‘From Wall Street to Web Street: A report on the problems and promise of the On-line Brokerage Industry’. This study suggests certain regulatory changes and addresses several problems that are plaguing the on-line securities business – chiefly IT and operational issues.

Regulatory policy initiatives

The SEC's key policy initiatives include the 'Operational Capability Rule' requiring brokers to have sufficient operational capability to conduct a securities business. This has been criticised by the industry for being too vague and not going far enough to define what 'sufficient' means. The vagueness of the Rule was probably deliberate, as the SEC wanted to "exercise caution by not dictating too specifically a systems standard for the industry." The Commission has accepted these misgivings and is evaluating several alternative approaches.

The SEC is concerned about the potential threats posed by conducting business on the Internet, while recognising the potential benefits to society. Therefore, it has so far steered clear of any especially onerous rules, preferring to focus on guidance, education and policing existing statutes.

Europe

Much of the regulatory response is being driven by the European Commission at a 'pan-European' level through directives covering distance selling, and privacy/data protection and the E-Commerce Directive itself, which seeks to establish an e-friendly framework for e-business.

At a national level the regulatory response has been mixed. The Swedish regulatory authority (Finansinspektionen), for instance, published a report entitled '2000:3 Internet and Financial Services' in April 2000 which covers:

- The development of Internet and financial services
- The Financial institutions and Internet
 - New possibilities
 - Dealing with risks
 - Marketing and consumer contacts
 - Steps taken by Finansinspektionen
- The Customers and the Internet
 - Security
 - Integrity
 - Support
 - Advisory services
 - Information
 - Certification of web sites
 - Virtual web
 - Regulations
 - Steps taken by Finansinspektionen
- The Internet and the EU
 - Suggested directives
 - Electronic signatures
 - Regulations and applicable laws

Speeches have also been used as a medium for delivering guidance to the industry and examples of topics addressed by the Director General of Finansinspektionen are:

- Operational risks in stocktrading through the Internet – response time and processing time in periods of intensive trading
- Concerns about the competence of advisers operating through the Internet
- Concerns about lack of objectivity in the marketing of shares, mutual funds and public offerings through Internet media
- Concerns about consumer protection in connection with Internet services

In the UK, the Financial Services Authority has issued guidance on the interpretation of its rules in an on-line environment and the need for management to address new risks inherent in such operations. There is no evidence of any fresh regulations in this area, although FSA's senior management have made keynote speeches regarding future developments in e-regulations. The FSA has initiated an assessment process for new entrants into this arena which includes close scrutiny of operational issues such as:

- Operational resilience
- Disaster recovery procedures
- Business continuity planning
- Internal security and change control management

The French Commission des Opérations de Bourse (COB) has issued non-compulsory guidelines outlining good practice for companies disseminating financial information on the Internet and for practitioners advertising and selling investment funds or portfolio management services on-line. In 1999, the French Conseil des Marchés Financiers, the self-regulatory organisation for stock markets and takeovers, set out revised rules governing the receipt and transmission of orders via the Internet. These regulations are an adaptation of the CMF's general guidance. The technical stipulations that had previously inhibited the full use of the Internet have been removed.

Asia-Pacific

The Australian Securities and Investments Commission (ASIC), the single national regulator of financial services, has been keen to develop specific policy initiatives for e-commerce in financial services. The ASIC could be characterised as a consumer watchdog rather than a guardian of systemic risks – the Wallis inquiry having explicitly made this distinction a few years ago. The ASIC sees the impact of new technologies as within its remit. Its approach could be regarded as investigative rather than prematurely prescriptive.

The ASIC's key priorities include:

- Focusing on achieving regulatory objectives rather than developing technological solutions
- Aiming to develop policies that are technology neutral
- Ensuring that regulatory requirements for e-commerce are no more onerous than those covering other distribution outlets, where this is consistent with good policy
- Ensuring that consumers using e-commerce have at least the same level of legal protection as would apply to other forms of commerce
- Pro-actively assessing the impact of technological developments on the efficiency, safety and equity of the financial system, including seeking input from industry when appropriate

In Hong Kong, the Securities and Futures Commission (SFC) issued its 'Guidance Note on Internet Regulation' in March 1999. The Note specifically requires registered persons to institute additional operational procedures for the conduct of securities trading over the Internet, including measures to safeguard the operational integrity of systems and strengthen security, reliability, capability and contingencies in the following areas:

- Suitability and general conduct requirements;
- Order handling and execution;
- System integrity;
- Responsible personnel;
- Written procedures;
- Client agreements
- Record keeping and reporting requirements.

The Note also addresses a range of related areas including:

- Risk disclosure
- Enforcement
- Issuing of advertisements or other documents relating to securities, investment arrangements and investment advisory services
- Offers of securities and investment arrangements through an electronic prospectus

A Steering Committee on the Enhancement of the Financial Infrastructure was set up in March 1999 to improve the financial infrastructure in Hong Kong. The Committee issued a report in September 1999, with a number of recommendations being implemented in 2000. The aim is the creation of an e-infrastructure which consists of:

- Single clearing arrangement
- Straight through processing
- Scriptless securities market
- Robust and scalable technology structure

The SFC's Internet surveillance program includes the daily monitoring of web sites, chat-rooms and bulletin boards, aimed at detecting any activities which target Hong Kong and which may infringe on legislation enforced by the SFC. In deciding whether or not Hong Kong is a target, the SFC will consider the nature of the business activity, as well as other factors, such as whether a local distribution agent is used, reference is made to Hong Kong dollars or Chinese language is used. If the surveillance reveals any potentially illegal activity directed at another jurisdiction, information concerning these activities will normally be passed to the regulator in the appropriate country.

In Japan, the supervisory authority has not been particularly active in the implementation of industry-wide rules or the passing of any pertinent laws and ordinances. In September 1999, the Japan Securities Dealers Association was established and released guidelines entitled 'Considerations In Regard to Internet Trading'.

While the Monetary Authority of Singapore (MAS) is currently understood to be drafting specific regulations on e-commerce or e-business activities for financial institutions, these are still under review. However, certain guidelines have been issued by the regulators covering the posting of financial product information on third party web sites and the offer of securities over the Internet.

Insurance

There is proportionally less Internet activity in the insurance sector than in the banking and securities sectors. Consequently, the regulatory response is not as developed. Many of the issues arising are generic across the whole financial services arena and similar regulatory responses to those seen above, particularly in the banking arena, are expected from insurance regulators as this market develops.

US

Little has been seen in the way of a formal regulatory response beyond any of the issues raised above. The main issue facing the US personal insurance industry predates e-commerce; namely that insurance providers require licences in each different US state. This barrier remains unresolved.

Europe

E-insurance is at a relatively early stage of development in Europe. With few insurance companies actually offering services over the Internet, no specific regulations have yet been formulated, though compliance with existing rules is expected. Many EU countries also require written proposal forms and other insurance contractual documentation for legal purposes. As long as other forms of validation, such as a digital

signature, are unacceptable, this will remain a barrier to the development of insurance on-line. Some countries are now looking at amending their legislation in this area (see Legal response to date).

The Comité des Assurances Européen (CEA) has welcomed the European Commission's latest draft directives covering such crucial areas as distance selling and electronic signatures, which aim to create a homogeneous and dynamic framework for the development of electronic transactions. However, insurers want the EC to ensure consistency between all community 'horizontal' initiatives under preparation or in course of adoption.

Asia-Pacific

There have been no significant initiatives by regulators in the region. In Hong Kong, the Insurance Association and the Information Technology Services Department are looking at ways of enabling insurance companies to accept returns submitted electronically, as outlined in the recent Electronics Transactions Ordinance.

Legal response to date

Legislators are addressing jurisdictional difficulties, though these remain serious concerns for the financial services industry as it seeks to develop e-commerce internationally. Global businesses complain that there is no coherence in the different regulatory frameworks around the world. Governments must strive for common standards and approaches if the innovative possibilities of the Internet in financial services are not to be stifled.

There has been some legislative progress in response to this challenge, notably the European Commission's (EC) E-Commerce Directive which advocates the 'country of origin' principle, an important step towards breaking down the jurisdictional barriers restricting the use of the Internet. The EC is also calling for the establishment of a framework for the recognition of electronic contracts formed on-line, putting an end to the outdated requirement to provide a 'wet' signature¹. In the US, most state law already recognises the validity of digital signatures on contracts and imminent federal law should see this concept adopted by the federal regulators.

However, jurisdictional boundaries continue to create uncertainty over key aspects of contractual law and financial services regulation. Failure to overcome such difficulties through harmonised standards will result in e-enterprises being forced to put up firewalls around their networks, in an attempt to contain and insulate one market and one set of market players from the wider international marketplace.

There are a number of specific legal issues central to the conduct of e-commerce which are being addressed by legislators around the world.

From a US perspective ...

Apart from the reform of digital signature legislation at a state level, very little pure reform has yet to be enacted. However, Congress is currently considering three bills dealing specifically with market data, namely S.95 – The Trading Information Act, H.R. 354 – The Collections of Information Antipiracy Act and H.R. 1858 – The Consumer and Investor Access to Information Act. The SEC supports H.R. 1858 but is yet to take a position on either S.95 or H.R. 354.

¹ The issues of trust associated with the use of digital signatures cover identifying the parties involved in the transaction, as well safeguarding business on-line from breaches of confidentiality or tampering with information. Public Key Infrastructure (PKI) which, with its various technology components, offers organisations a solution to mitigate, if not alleviate, the evolving levels of risk.

One of the most crucial pieces of recent US financial services legislation is the Gramm-Leach-Bliley Act (GLBA), which has transformed banking regulation. Enacted in November 1999, the GLBA removes barriers which had previously prevented financial services providers from offering seamless services. While it does not address e-commerce specifically, the core privacy protections in Title V of the GLBA arising from the sharing of customer data, have important implications.

The GLBA applies to all financial services, regulated and non-regulated, as well as any operation of a financial nature or incidental to financial activity. The Federal Reserve, OCC, NCUA and FTC have all issued fresh guidelines in response to the Act, with the SEC set to follow. The state regulatory agencies will be responsible for issuing new codes for insurers.

GLBA requires:

- Financial institutions to develop and disclose privacy policies and statements. This policy should be disclosed on the establishment of the relationship and then annually for all the institution's customers.
- Financial institutions not to share customer data with non-affiliated third parties for marketing and other purposes not related to the administration of accounts.
- Financial institutions to provide notice to customers prior to sharing information with third parties and the chance to opt out of such an exchange. It is important to note that in this context a 'customer' means the institution's customers, along with individuals from whom personal data has been collected but who do not have a customer relationship with the institution.

Although the scope of the GLBA is vast, it does not pre-empt state regulation. Some states are planning even tougher privacy protection such as restricting affiliate sharing. It is believed that one reason for this is that the GLBA fails to meet wider international standards of protection such as the EC's 'safe harbour' proposals .

From a European perspective ...

In Europe, legislators are focusing much of their attention on the issues surrounding the passporting of services, particularly in banking. Home versus host state supervision is an especially vexed question. Institutions may seek authorisation wherever tax, compliance and costs are lowest, once cross-border trading makes operational location less critical. Therefore growth in e-banking is likely to lead to a significant increase in the use of the 2BCD passport and growth in on-line brokerage will have the same effect on the use of the ISD passport. This will make it even more crucial for European regulators to undertake supervision in a satisfactory – and by implication harmonised – manner and to ensure that that communication between regulators is adequate.

A number of initiatives with implications for home and host state supervision are under discussion, including draft e-commerce and distance marketing directives, as well as the Rome and Brussels Conventions. The debate is far from being resolved and a degree of confusion remains. For example, the E-Commerce Directive aims to provide legal certainty as to the place of establishment of an Internet service provider. While this may not necessarily be the place where web sites or servers are located, operators will be subject to the regulatory regime of the EU member state where they are established. However, the drafting is sufficiently vague as to open up the possibility of numerous regulators asserting jurisdiction over an Internet service. It is essential that European regulators agree on a suitable compromise; otherwise, they could nullify home state supervision, the main advantage of the Directive.

At the same time, the Directive requires individual countries to remove any restrictions on the use of electronic contracts. In particular, this would include the repeal of any curbs on the use of electronic media

or any legal differentiation with other forms of contract. Significantly, it also states that Internet service providers will not be liable where they have acted as 'mere conduits' for information from third parties.

In November 1999, the EC adopted the Electronic Signatures Directive, aimed at creating a harmonised legal framework for electronic signatures in the EU. The Directive introduces the concept of certificates and certification service providers for the verification of digital signatures. All member states must also recognise the validity of such signatures as confirmation of a contract or their admissibility in evidence.

The Electronic Communications Act, which will implement the Directive in the UK, will include the recognition of electronic signatures. However, there are still certain documents that are by law required to be either 'in writing' or 'signed'. It remains to be seen whether electronic signatures would be allowed in such circumstances. Also, while the electronic signature will in principle be admissible in court, it will ultimately be up to judges to decide on a case-by-case basis. The Act will also open the way for secondary legislation to impose conditions on the required electronic form of a communication. There is currently a vast amount of legislation demanding, or that could be interpreted as requiring, paper records, and this will allow for clarification.

Equally complex are the restrictions on cross-border flows of personal data. Such data is defined as information that could identify or lead to the identification of a particular individual. Until recently, the various countries of the EU maintained different levels of legal protection for personal data. In the UK, for example, national safeguards were enshrined in the 1984 Data Protection Act. In 1995, the EU adopted a new Data Protection Directive² which later formed the basis of the UK's updated 1998 Data Protection Act. One of the key features of this new European regime is the restriction on transfers of personal data out of the European Economic Area (EEA). Data cannot be passed to a country or territory outside the EEA unless there is deemed to be an adequate level of protection. Accordingly, when dealing with countries from outside the EEA, data protection issues must be considered on a case-by-case basis.

There are a number of other areas relating to e-business which call for further legal clarification and, in some instances, more definitive legislation. These include the timing and method of contract formation in the on-line arena, the liability of intermediaries (such as Internet service providers and network access providers) and, crucially, the determination of laws applying to a particular transaction. On a European level, the E-Commerce and Electronic Signatures Directives tackle these (and other) issues. However, these will now need to be enacted in each member state which, in turn, may lead to inconsistencies between jurisdictions. In addition, harmonisation with non-EU countries is vital.

'eEurope 2002, an Information Society for All', which was approved at the Lisbon Summit of June 2000, marks the way forward. It aims to accelerate Europe's legislative programme regarding the Internet and e-commerce and break down any national 'barriers to entry' in this area by 2002. The Summit concluded that all EU countries should enshrine this legislation in domestic law by 2001. Ireland and Germany are currently drawing up bills or amending existing legislation to take account of this and other recent EC directives.

However, in its desire to create an e-friendly environment, there is a school of thought which says that Europe is actually in danger of over-regulating e-business and handing a competitive advantage to US companies. Striking the balance will clearly be difficult, especially as government responsibility goes beyond guarding against crime and protecting consumers, into such equally uncharted waters as collecting on-line taxes.

² The EU Data Protection Directive radically overhauls the existing European data protection regime. The Directive restricts the transfer of personal data to countries outside the European Economic Area, unless there is an adequate level of protection in the destination country. As the US does not have comprehensive national data protection legislation in force, the level of protection can vary from state to state. The 'safe harbour' system is a system whereby companies in the US would commit to a set of privacy principles and thereby meet the EU's requirements.

In addition to directives addressing on-line issues, the Investment Services Directive is also under review as part of the European Commission's 'Financial Services Action Plan'. The most significant matter under debate for the on-line community is an issue the European Shadow Financial Regulatory Committee has described as a "key weakness of the ISD." This is the so-called 'regulated markets' concept which, as things stand, may be used by national authorities as a protectionist weapon for their domestic markets. Reform in this area is likely to have a major impact on the European market infrastructure. It is also likely to make passporting under the ISD a key issue in competition between European markets and exchanges.

Elsewhere in the world ...

As previously discussed, many countries in the Asia-Pacific region, such as Australia and Hong Kong, have strengthened their safeguards on privacy. There have also been some welcome developments in digital signature law, with Australia, Singapore and Hong Kong all passing electronic transaction ordinances.

In July 2000, Singapore became the first country in Southeast Asia to provide a specific legal definition of the rights and responsibilities of all parties involved in e-commerce. The Electronic Transactions Act aims to provide a safe and secure environment for e-transactions.

Hong Kong is about to follow suit through its Securities and Futures Bill, which aims to establish a regulatory framework for the development of a fair, orderly and transparent market. Underpinning the drafting of the Bill has been the need to match local priorities with standards capable of being compatible with the international marketplace. With regard to electronic trading, it seeks to create a flexible and pragmatic basis for the regulation of automatic trading systems. This includes giving the SFC the power to examine each ATS application and determine which specific rules are to be applied. Providers of ATS services will either be licensed as intermediaries or authorised like exchanges, depending on the nature of their business and operations. The objective is to afford a reasonable degree of protection to investors without holding up market development.

Overview

The advent of e-business has given rise to very few specific changes in regulation or modifications in the ways regulators regulate. From a retail perspective, the spotlight has largely focused on educating consumers. For example, the SEC recently launched an investor education web site, as well distributing free publications which outline how the industry works and the best way of avoiding fraud. Other initiatives include 'town meetings' where investor concerns are addressed and advice offered on how to plan a secure financial future. The SEC works with regional and national media to help publicise its various programmes. It is clear, however, that while consumer education has been placed high on the list of priorities, perception of its value varies. The US authorities, for instance, prefer to combine such initiatives with public, on-line, enforcement action against those that break the law and those that flout its rules.

The US has also seen the only real evidence of regulators themselves embracing the technology, with particular examples including:

- Receipt of regulatory information directly from or via the regulated firm itself
- 'Real time' surveillance of the markets to monitor the positions and exposures of regulated firms
- 'Real time' surveillance of the markets to monitor trends and predict problems enabling effective deployment of the regulatory resource
- The use of market and analyst information on the firms themselves

Summary

The general approach adopted by regulators globally can be summarised as follows:

- Regulators are almost universally relying on the issuing of guidance as the main way of promoting compliance within an e-environment. Regulators are looking to the markets and market participants to set and enforce high standards of fairness, efficiency and safety. This gives the industry an ideal opportunity to influence the nature of future on-line regulation. It also places particular responsibility on senior management to ensure this is achieved and, indeed, highlights significant risk if they get it wrong.
- Regulations will remain largely technology neutral and existing rules should be applied by regulated firms to their e-businesses. The SEC has started to focus on new regulatory issues arising from the rapid growth in e-commerce such as suitability requirements, after-hours trading rules and best execution. We envisage that emerging e-economies will have to follow.
- Guidance, from a rules perspective, is limited and firms are often required to make their own interpretation.
- Antiquated paper-based record keeping and wet signature requirements are being eliminated where possible, though this often requires amendment to existing legislation.
- Increasingly, systems issues are being seen as the greatest threat to investor protection in an e-environment and these are receiving even more regulatory scrutiny. These issues include data protection, security of information, operational resilience and business continuity planning.
- No formal change to capital adequacy requirements is proposed at present in connection with the delivery of IT dependent services. The increasing focus on operational risk within the Basel Committee's proposed capital adequacy requirements has not singled out e-banks as requiring higher levels of capital. However, such requirements cannot be ruled out as the development of operational risk frameworks gains momentum.
- Regulators are recognising the need to review regulatory objectives in line with the changing market infrastructure created by disintermediation and consolidation in the industry.

What are the future challenges for regulators?

'The continuing transition to electronic trading, both domestically and across international borders, is fuelling significant changes in capital market structure and participants' roles. While these developments deliver greater efficiencies and new opportunities for market users, they also raise significant issues for regulators. There is an important balance the FSA needs to strike between ensuring that regulation does not unnecessarily impede competition and innovation, and addressing any new risks arising from change.'

UK Financial Services Authority

Regulation of the access points or 'gateways' to the Internet has been suggested in the past – i.e. regulation of the Internet Service Providers ('ISP') – as a means of regulating, at source, the provision of content and information available to the public. It seems unreasonable that an ISP should be made responsible for the information it carries merely by virtue of its role as a conduit. Indeed, current thinking behind, for instance, the European Commission's Electronic Commerce Directive reinforces this. The alternative is to give the ISPs regulatory responsibilities of their own, i.e. to force them, in effect, to act as self-regulatory organisations. This seems highly unattractive for the ISPs and thus impracticable to implement. We, therefore, conclude that regulation of the market participants themselves should continue with the Internet treated merely as a new delivery medium. This approach has found favour in law, as well, where recently the US Supreme Court, in *Lunney v Prodigy Communications*, let stand without comment a New York ruling that Prodigy was not legally liable for objectionable e-mail or bulletin board messages it carried as an Internet service provider.

Throughout the developed world, financial services regulation is applied for the reasons already stated. Whilst the approach of regulatory bodies varies quite significantly, and the structure of regulation varies in terms of who regulates, the way in which regulation is applied is fundamentally the same. That is that a financial services (banking, insurance or securities) provider must be authorised/approved before commencing operations and that, once authorised, providers are supervised to ensure compliance with the rules and disciplined through enforcement action when they do not.

The 'rules' themselves are applied through prudential and conduct of business regulation. Banking and insurance regulation is founded on safety and capital adequacy and is generally applied at a prudential level only. This means strict capital adequacy requirements and ongoing assessment of management, systems and control.

In the last section we identified some of the new regulatory issues facing the industry and its regulators and summarised the regulatory response which varies from country to country, dependant upon the maturity of its financial services e-commerce industry. Whilst the regulatory response has generally been positive and informed, it has tended to be reactive rather than proactive and there is a need for a more proactive response to address areas of uncertainty for the industry and enable it to deliver equivalent investor protection in the on-line environment.

We now look at the process of regulation and, more specifically, at the new issues that e-commerce raises from a regulatory perspective, how regulators should set about addressing these, where change is required, and why.

How should e-commerce be regulated?

This paper addresses the regulation of financial services delivered via e-commerce, not regulation of the delivery medium (i.e. the Internet) itself. Regulation of the medium itself is impracticable due to its size, diverse nature and multiplicity of jurisdictions.

Securities and investment business regulation, particularly in the retail sector, is a combination of prudential and conduct of business requirements. In addition to the prudential issues raised above, this means that such firms have to comply with detailed rules regarding the way in which they conduct their business.

It is our belief that this core framework for regulation remains valid in an on-line environment, subject to it being applied at a global level, where this is appropriate and achievable. The issues that arise, and that are raised in this paper, span both conduct of business and prudential regulatory requirements. In terms of the way that regulators regulate, the process shows little sign of changing from that of authorisation, supervision and enforcement.

New issues arise, however, within these frameworks and Tables 4.1 and 4.2. summarise how examples of these may have an impact within the current regulatory framework.

Table 4.1

Authorisation	Supervision	Enforcement
<ul style="list-style-type: none"> Regulators increasingly see consideration of IT competence as a key part of their 'fit and proper' assessment. Banking authorities are being forced to view critically the commercial viability of the on-line banking sector in its consideration of the authorisation of further e-banks. Pre-opening examinations are undertaken by US banking authorities. Banking supervisors demand that technology costs be capitalised upfront. 	<ul style="list-style-type: none"> Group supervision techniques are increasingly going to be required as financial service providers are no longer likely to fit into convenient 'silos'. On-line (potentially, 'real time') supervision by regulatory authorities will, increasingly, become a part of the regulators 'tool kit'. 	<ul style="list-style-type: none"> US cease and desist orders could, theoretically, be less successful as they depend upon expert evidence which, in many cases, is difficult to find. Power is being exercised more stringently by banking supervisors if management allow the business to operate 'outside' the scope of the original business plan.

Table 4.2

Prudential issues	Conduct of business issues
<ul style="list-style-type: none"> Management responsibilities arising from the launch of a new on-line business The impact of IT dependency on operational risk and, therefore, capital adequacy requirements 	<ul style="list-style-type: none"> Know your customer Consumer education Marketing Suitability Privacy Best execution E-offerings
<ul style="list-style-type: none"> Management of IT capability 	
<ul style="list-style-type: none"> Cross-border regulation 	

The challenges

The phenomenon of the Internet and the applications that have been developed for it present unusual challenges for the regulators. This is because:

- They will have to introduce regulation that will facilitate the further growth of this phenomenon and its applications.
- Paradoxically, the growth of the applications and the constant development of new information systems may force regulators to review any regulation and update it, as appropriate, continuously.
- The Internet is a global phenomenon and e-commerce spans different jurisdictions; successful regulation will be that which is consistent at a global level.

So, how should these issues be addressed?

The role of the industry

The role of the regulators should continue to be to ratify and enforce good market practices ... This creates unprecedented opportunities for the financial services industry to affect the development of policy, and enormous risk if its constituents remain on the sideline.

It is our belief that management of the key threats and concerns is largely a governance issue for the industry and that good market practice will effectively produce an environment of self-regulation that will address many of the issues that have arisen. The role of the regulators should continue to be to ratify and enforce such practices and, only in the case of some extreme issues, bring an independent perspective to the party where intense competition is restricting the development of good market practice.

This is a debate that is in its early stages and the regulators, internationally, are clearly seeking input and guidance from the industry. This creates unprecedented opportunities for the

financial services industry to affect the development of policy and enormous risk if its constituents remain on the sideline.

In the next chapter, we consider how management in the industry may respond to these challenges. Reference should also be made to Appendix 1 of this report, 'To be in (e)-business tomorrow, what should financial services companies be doing today?'

The role of the regulators

The regulators can address these challenges by:

- Reviewing, on a regular basis, their regulatory objectives in the light of a rapidly evolving market.
- Resisting the temptation to over-regulate while nevertheless ensuring that 'fit for the purpose' IT standards are adopted globally. There is a lot of hype that could lead to a knee-jerk reaction. The basic principle of differentiating between retail and wholesale activity should be applied equally in an on-line environment ensuring that B2B activity benefits, where appropriate, from 'lighter touch' regulation.
- Addressing the key jurisdictional difficulties that arise from a national regulatory framework being used to regulate this global medium.

- Reacting quickly to new regulatory challenges and risks with changes in regulatory practices and rules where appropriate. Such action is likely to be required in the following areas:
 - Conduct of business regulation
 - Prudential regulation
- Using the technology to improve regulatory processes and to equip supervisors with the necessary tools to regulate e-businesses effectively.

Regulatory Objectives

We have already determined that many national regulators have started addressing a number of these issues. The regulatory approach should be embodied in objectives set specifically for the competent regulation of financial services over the Internet. These should include:

- Not stifling innovation
- Improving consumer education and understanding
- Avoiding over-regulation – letting self-regulation through commercial demands and industry standard-setting run its course
- Pursuing international co-ordination, co-operation and consensus with the utmost urgency
- Ensuring that satisfactory standards of IT competency are maintained within regulated firms and that investors are not prejudiced through unavailability of service
- Utilising technology wherever possible to make regulation more efficient and less costly for market participants and, ultimately, consumers

We now consider these proposals in greater detail.

Jurisdictional difficulties

If national legislation is not to restrict the development of e-commerce activity, global agreement must be targeted as a means of facilitating international on-line activity. The end result must be an environment where there is certainty in terms of the application of law and regulatory requirements. This could take a couple of forms:

- Global regulation through the country of origin principle as proposed in the European E-Commerce Directive. This is clearly an ambitious target and would require, as a minimum, general agreement between the G10 countries. In reality, whilst attractive to the industry, it is unrealistic for legislators to devolve responsibility for protecting their citizens to the law makers in another country. Whilst potentially achievable from a regulatory perspective, the issue of contract law is far too deeply enshrined in national legislation to work in practice.
- The creation of 'safe harbours' which means that, whilst regulation continues to take place on a jurisdictional basis, compliance with certain minimum standards, rules and principles will ensure that business can be undertaken globally without the need for separate authorisation in each jurisdiction.

The first, welcome step taken by the major global regulatory bodies is the 'targeted at' principle. The Internet would be prohibitive as a medium for the delivery of financial services if every national regulator required every on-line financial services provider to be authorised under its domestic law and to comply with its advertising rules. An increasing number of regulators have announced that they will not seek to apply their enforcement powers to web sites that are not targeted at residents in their country. This, however, is equivalent to 'scratching at the surface' of the problem. The real problems start when a firm does wish its services to be 'targeted at' citizens outside its own country. The firm suddenly enters a world of different contract and financial services legislation, different regulatory rules, and it needs to be separately authorised in each one. Furthermore, a plethora of tax issues arises.

Financial services regulation is not unique in its failure to keep pace with the increasing globalisation of business today but that does not mean that it should not already be tackling the issue at a global level.

There is clearly a need for global harmonisation of legislation dealing with e-commerce. However, given the time it has taken the EC to produce the legislation we have referred to in this document (despite it being placed on 'fast track'), the prospect of concluding similar provisions on a global scale seems remote. More realistically, one might expect more limited global protocols to be agreed, similar to those which exist in relation to money laundering, at least as a starting point.

This could be extended to provide 'safe harbours' for e-commerce conducted in accordance with defined standards and possibly, given time, to a full code of conduct/legislative framework to which countries could sign up.

There is already recognition at an international level regarding the importance of this issue and IOSCO, in particular, has been the forum through which the issue has been addressed. However, whilst commitment to addressing the issue has also been forthcoming, this appears to focus far too much on enforcement i.e. punishing those that get it wrong, rather than addressing the real issue which is restricting legitimate financial services providers' ability to participate in a truly global marketplace. It is also discriminative to new market entrants, thereby creating higher barriers to entry to the global marketplace. Existing, large, international businesses will have 'acquired' a multiplicity of regulatory approvals throughout the world over a number of years which can now be leveraged to support new e-businesses. It is virtually impossible for a new entrant to replicate these within a reasonable time frame.

There are no easy answers to the jurisdictional challenges and these suggestions are merely a starting point. It will be interesting to see how this issue develops in practice.

The IT challenge

In view of the potential risks to both investor protection and the integrity of the financial marketplace, it could be argued that regulators should start setting minimum IT standards in areas such as:

A 'one-size-fits-all' approach to the area of IT standards would be inappropriate as different on-line service offerings require different IT standards and the aim should therefore be IT systems that are fit for the purpose.

- Business continuity planning
- Disclosure regarding systems performance
- Encryption
- Security
- Privacy

However, such an approach would require detailed guidance and/or rules to be drafted, the implementation of which would then need to be supervised. It is our belief that the regulators have neither the resources, nor the expertise, for this approach.

Moreover, a 'one-size-fits-all' approach to the area of IT standards would be inappropriate as different on-line service offerings require different IT standards and the aim should, therefore, be IT systems that are fit for the purpose.

This is the most significant area where the industry can apply a process of self-regulation. Individual service providers should be required to set their own minimum IT standards which, in appropriate cases, can be discussed and agreed with their regulatory bodies. Service providers should also be encouraged to share IT performance with consumers enabling them to take account of this key issue when choosing an on-line service provider.

Following, and assuming, establishment of the Regulatory objectives detailed above, we anticipate three key areas of further regulatory development in the future:

- Electronic reporting and monitoring
- Conduct of business and market conduct rules
- Prudential regulation

Electronic reporting and monitoring

Internet technology can be used as a means to improve compliance monitoring within regulated firms and, indeed, will be used to improve supervisory processes within the regulatory bodies themselves.

The majority of information received by regulators is historical, usually focused around month-end returns. Specialist tools can now be developed, using the new generation of Internet languages, to receive and monitor 'real time' or near 'real time' data and to identify trends or exceptions. Such tools can be automated to a very high degree. In the medium term, these will offer a powerful regulatory tool to monitor an individual company's compliance with certain rules in 'real time'.

As well as presenting challenges to the industry, therefore, the Internet must be seen as presenting exciting opportunities. The regulators are already looking at ways of utilising the speed and flexibility of the Internet for monitoring purposes and the regulated community should be doing the same in order to enhance existing monitoring programmes and to ensure that their own e-commerce activity is monitored in the same way as other activities.

Regulators are considering the incorporation of technology-based monitoring into their supervisory activities through the application of compliance software and the receipt of 'real time' execution information. This will involve setting new standards and incorporating new techniques for regulatory desk-based supervision.

The issues to be considered by the industry, therefore, are:

- Setting new standards for internal compliance monitoring using Internet technology.
- Using software in compliance monitoring.
- Getting the partnership right between regulators and regulated firms, i.e. the Internet is a monitoring tool which also, subsequently, provides a gateway to regulators for supervisory purposes.

What tools will the regulators (need to) develop?

In addition to the monitoring techniques mentioned above, we anticipate developments in the following areas:

- Policing the parameter – the key here is third party encryption or, for instance, use of such services as PricewaterhouseCoopers' WebTrust to equip consumers with the necessary tools to differentiate between the 'good guys' and the 'bad guys'. Additionally, the FSA in the UK, for instance, has recently stated its desire to pursue partnerships with the operators of search engines to recognise only financial services sites with a uniformly recognisable web site address such as xxxxx.finserv.co.xxxx. Only authorised firms would be able to use such addresses. The advantages of such web hallmark schemes include:
 - Improving customer awareness of the regulatory 'brand', and helping investors to conduct searches based on regulated companies only.
 - Ensuring regulated firms display the regulator's 'brand' and link to the local regulator's web site, where consumers would find a list of authorised companies.

- Educating consumers. Education is an essential aspect of investor protection, and electronic networks are well-suited to help provide comprehensive and up-to-date information and advice. It is important that investors are aware of these risks and how best to avoid them.
- Commencing on-line communication with firms to facilitate regulatory reporting and regulatory approval applications in particular.
- Using 'real time' data to improve monitoring of compliance in areas such as:
 - Best execution
 - Suitability
 - Cancellation rates
 - Insider dealing
 - Market manipulation

How could the regulators do this?

As stated above, much of the information received by regulators is historical, usually focused around month-end returns. Regulators supplement this information with client visits and external auditor reviews of compliance annually.

Regulators, like other users of financial information, need to be able to identify exceptions so that available resources can be directed in the most efficient manner. XML (see Appendix 3) and its derivatives will bring a much greater degree of access to financial data, including individual pieces of financial statements, but, being extensible, does not inhibit the information providers in the way that standard forms tend to produce constraints.

Specialist tools can then be developed to monitor the data across all entities or for an entity across a number of reporting period to identify trends or exceptions. Such tools can be automated to a very high degree where they operate on such highly consistent data.

In the medium term, such languages could offer a regulator a powerful tool to monitor an individual company's compliance with certain rules in 'real time'. For example, stockbrokers, under the conduct of business rules, are required to purchase shares for customers at the best prevailing rate at the time of execution. XML would allow the regulators to compare prices struck by a company with current market rates from other reliable sources, such as Extel. All breaches could be notified immediately and automatically to the regulators, saving time and effort by rectifying a problem before it escalates.

More generally, 'real time' monitoring of companies could lessen cyclical reporting constraints for companies, reducing the need for inspection visits and audit reviews. There are additional benefits through increased speed of monitoring which is becoming necessary to keep up with the pace of modern electronic business.

The increasing use of this type of language seems inevitable in the financial services market, driving greater transparency. Regulators will, in turn, realise the potential uses of the software and employ them in their forthcoming initiatives. Therefore, discussion over the timing of information extracts is needed. At this time, the debate over 'real time' monitoring is still in its infancy and the industry is in a strong position to steer future methods of rule enforcement.

Our key conclusion is that businesses must anticipate these developments by improving their own on-line internal monitoring. Therefore, if and when on-line monitoring does arrive, they will be fully able to operate effectively in this new environment. This has the added benefit of enhancing the effectiveness of internal regulation, with knock-on benefits for the company's reputation, client relationships and regulatory relationships.

Conduct of business and market conduct rules

When considering the conduct of business issues relating to e-commerce, regulatory action must differentiate between the retail and wholesale markets (where the issues are quite different as highlighted in Table 5.1)

Table 5.1

Retail	Wholesale
<ul style="list-style-type: none">• Customer understanding (armed with accurate business and product information and comparisons, consumers are able to make better informed purchasing decisions. However, in some instances, this flood of information can be confusing and consumers may have no effective means to verify its accuracy)• Know your customer requirements• Privacy• Suitability• Advertising and marketing	<ul style="list-style-type: none">• The availability and supply of market data• Dispersal of liquidity• The regulatory approach to outsourcing• Systemic risk issues• The role of markets and exchanges and their interaction with and dependence on participants

The greatest challenge in terms of rule-making certainly applies in the retail sector, where conduct of business rules have been drawn up essentially to cope with the pre-electronic age. Regulators throughout the world are already addressing changes needed to the conduct of business rules, but there is a long way to go in terms of considering what notifications, risk warnings, 'reasons why', projections, cooling-off periods and suitability requirements should apply in respect of transactions through the Internet.

Equally, the use of artificial intelligence to respond to investors' queries and applications presents a further challenge to ensure that those artificial intelligence systems are adequately programmed and regularly updated to take account of developments in the market.

These issues will be particularly relevant to financial services companies as they seek to put increasing proportions of their business through the Internet, saving significant selling and processing costs, but potentially incurring significant operational risks.

Faced with questions about accuracy of information, contract formation, availability of redress and dispute resolution mechanisms and the potential for fraud and privacy issues, investors are concerned about the practicalities and the safety of the electronic environment and many remain reluctant to participate fully in electronic commerce. Investors need assurances that the electronic marketplace provides a safe and predictable place for them to do business.

At present, regulators are generally more concerned, and thus occupied, with 'policing the perimeter' (i.e. keeping the unregulated from defrauding their consumers) than they are with changing their approach to the regulation of legitimate Internet activity. The ways in which this is achieved vary by jurisdiction, but include specific attention to the education of consumers and enforcement action against unregulated entities where achievable.

The way forward

Our overall view is that, in the conduct of business area, there is an existing body of regulation that is valid and applicable, and the need for specific regulatory rule changes, at a national level, is minimal. The rules are antiquated, however, in certain areas and some changes, therefore, need to be made. There are specific areas of concern within the industry which are caused either by a lack of certainty regarding the interpretation of rules in an electronic environment or by the restriction of innovation caused by the outdated nature of the rules themselves. The challenge to the industry at present is to interpret existing rules and regulations, address new risk issues and deliver compliance.

For instance, the most recent message from the UK regulatory authorities, accompanying guidance on the above issues, states:

“... (the) approach in the area of electronic commerce remains the same; namely that conduct of business rules are drafted at a sufficiently high level of generality to allow them to apply to firms’ activities in the area of electronic commerce.”

IOSCO guidance to regulators as far back as September 1998 said that regulators should give guidance to the market on the application of their rules in an e-environment. Whilst there is increasing evidence that regulators are addressing this need, there remains an urgent need for additional guidance from regulators regarding the application of their rules to bring regulatory certainty to the conduct of financial services over the Internet.

Areas in which such guidance/new rules are either impending or required, include:

Rules

- Take conduits outside the scope of regulation – particularly relevant in the case of portals
- Recognise IT based record-keeping and allow client information to be held in electronic form only

Guidance

- Recognise new issues arising as a result of advertising on the Internet, particularly in the context of hypertext links
- Clarify regulators’ expectations of suitability investigations, particularly in respect of data profiling of clients and day trading
- Define, where applied, minimum standards relating to IT capacity and back-office processing power
- Clarify the expectation of firms regarding the privacy of client information
- Clarify best execution requirements in a on-line fragmented market
- Define account opening and anti-money laundering requirements
- Clarify rules relating to electronic communications

We now look at some of the key conduct of business issues and, where appropriate, discuss how these might be resolved.

Money laundering

The shift in the nature of the industry has added a new dimension to the legal requirement that firms verify the identity of their customers for anti-money laundering purposes. As there is less face-to-face contact with customers, standard procedures for verification (for example passports or national identity cards) may no longer be appropriate. Any mechanism which avoids face-to-face contact with customers can provide

additional opportunities for criminals to gain access to the financial system and, therefore, creates new challenges in electronic verification of identity. Institutions will be required to move away from paper-based verification and documentation towards electronic types of verification of identity. There are some real challenges in this area, not as yet fully explored, and the use of biometric security features such as digital voice recognition and thumb print analysis may well play an important part in future financial services practice.

There are considerable challenges ahead for the financial services industry. Institutions must continue to guard against the reputation damage of being associated with a major money laundering scandal and meet increasingly onerous regulatory requirements. In this rapidly developing environment, it is vital that regulators adopt a pragmatic approach to the interpretation of money laundering rules, in order that they are an effective deterrent to serious crime without becoming an unnecessary burden on the financial industry. Therefore, a regime that evolves to meet the needs of a rapidly changing financial services sector is imperative.

Consumer education

Most modern financial services regulation, whilst focused on providing investor protection, is based on a basic principle – caveat emptor. There is no reason why consumers should not take responsibility for their

'If it looks too good to be true, it probably is ...'

own on-line buying decisions. However, they need to be properly equipped to make such decisions. The regulators have sought to educate through their own web sites and 'roadshows' – it is now up to the industry to follow suit. There is increasing evidence that many responsible financial services providers are already addressing this issue recognising that, like most

regulatory requirements, there is also commercial advantage in having knowledgeable customers as they are likely to buy sensibly and, thus, come back again and again.

Ways in which financial services companies may address this issue include:

- Working with the regulators to initiate joint-funded education campaigns
- Providing hypertext links to domestic regulatory web sites
- Ensuring relevant risk warnings are prominently displayed on web sites
- Supporting the existing and ongoing regulatory initiatives in this area
- Providing investors with the opportunity to trial services in a non-live environment
- Incorporating e-mail advice into the account opening process, including:
 - The need to make investment decisions in the same way as in an off-line environment
 - Recommendation that independent investment advice is sought, where appropriate
 - Advice regarding the regulatory protection offered within the jurisdiction in which the service provider operates and the compensation scheme applying
 - Identification of the risks, where these exist, of buying over the Internet and how these should be managed by the 'buyer'

Privacy

The regulators are faced with a challenging conundrum: if they increase the legislation in this area, they are likely to hamper the advancement of Internet applications in the financial services industry. On the other hand, if they do not provide a framework to ensure the safekeeping of data, the risk of infringing the human right to privacy increases.

Possible consequences of a privacy failure include:

- Damage to brand, reputation, consumer retention and customer-focused business strategies
- Loss of revenue and new business

- Possible regulatory enforcement actions – millions spent and loss of flexibility in marketplace to implement consent decrees
- Potential litigation from consumers, advocates and business partners
- Civil and criminal penalties for wrongful disclosure of protected health information
- Interruption of cross-border data flows with applicable penalties in international jurisdictions

Although there have been advances in respect to the management of information, the rules should be consistent globally without being too onerous on the institutions.

Advertising and marketing

The whole area of marketing and advertising has also risen to the top of the agenda as the high cost of recruiting on-line customers and the extremely competitive nature of the market have resulted in aggressive advertising campaigns. The two main issues/concerns are:

- On-line advertising
 - Transparency.
 - Hyper-text links.
- Off-line advertising
 - There are doubts about the ethical nature of advertising which encourages a culture based on speculative trading rather than investment for the long term. Day trading is a prime example of this, which, it could be argued, has as much in common with gambling as it does investment.
 - The expectation gap.

Added to all this is the trend in data mining to target investors with automated market information in an attempt to encourage trading and thereby increase volume.

The regulatory authorities have identified these issues as areas of concern although action taken has been limited. In Europe, the European Commission has drafted and consulted on the Distance Selling of Financial Services Directive. The Directive seeks to establish a legal framework governing the distance marketing of financial services with the specific goal of increasing consumer confidence in the use of new techniques. It covers contracts for which the supplier exclusively employs means of distance communication and it aims to contribute to the development of electronic commerce.

The proposed measures seek to provide a high level of consumer protection. A right of withdrawal and a reflection period are introduced and the information to be provided in the contract is regulated. One article is devoted to out-of-court complaint and redress procedures. With a view to ensuring the free movement of financial services, a maximal harmonisation approach is adopted: member states may not adopt provisions other than those laid down in this directive in the harmonised fields.

The European approach, whilst sound in its content, appears heavy-handed as it requires member states to incorporate the Directive into domestic legislation. This is, again, an area that the industry could lead through the adoption of best practice, incorporating:

- Cooling off periods for long-term retail investment products
- Avenues for dispute resolution arising from on-line business
- Full transparency in terms of the 'offering' service provider, the product(s) being offered, full terms and conditions, the identity of the providers' regulator(s) and the compensation scheme applying (if any) if a transaction is undertaken

Electronic communications

Clarification is required in terms of what is meant by 'written notice' or written agreements under existing rules. E-mail should be considered sufficient for 'notice' requirements whilst electronic agreements should be recognised where enabling technology such as digital signatures facilitates this.

Prudential regulation

Some would argue that the financial services industry has been slow to understand the potential of the Internet and have delayed going on-line through fear and ignorance. There is increasing evidence, however, that this reluctance is now being overcome and the industry must ensure that its back and middle office processes keep pace with innovation in the front office and maximise the potential offered by new technology.

We anticipate further developments in the following key areas:

- The impact of IT dependency on operational risk and, therefore, capital adequacy requirements.
- Management responsibilities arising from the launch of a new on-line business. Increasingly the burden of regulation is shifting to the management of regulated firms. We refer in the next chapter to the issues requiring specific management action so as to handle the risks now forming part of e-business.

Operational risk

Regulators have always been concerned about risks other than purely financial risks such as credit and market risk. It has long been a requirement that financial firms should have adequate systems and controls. However, firms and regulators are now specifically developing tools to capture the risk of financial loss that such risks, including operational risk, create. Dependency on IT systems, which e-business can only exacerbate, is clearly a source of such risk.

Hitherto, in the face of the difficulty of accurately measuring the risk of financial loss caused by other risks, the supervisory approach to non-financial risks has been purely qualitative. The June 1999 consultative paper from the Basel Committee on Banking Supervision foreshadowed the application of capital requirements in respect of 'other risks', in addition to the application of higher capital requirements to institutions whose risk assessments showed them to be more risky – an assessment which would include IT capability. This was taken a controversial step further forward in the November 1999 consultation by the European Commission which sought views on a methodology that used balance sheet size and non-interest income as a proxy basis for applying a minimum capital charge.

While the European Commission's proposals, in particular, have generated a hostile reception from the industry and leading commentators, it is clear that, in the not too distant future, IT vulnerability will be penalised both by increased capital requirements and by increased intensity of supervisory attention.

Management of IT capability

Appendix 1 contains further comment on the subject of IT capability. Management responsibility is very much focused in this area and a fine example comes from the US – in anticipating a surge of new technological financial products about to offer consumers direct interactive access to US banks, the Board of Governors of the United States Federal Reserve System (FRB) has expressed its concern regarding the

new levels of bank security that will be required to protect both customers and banks. Specifically, the FRB stated that,

“the Board also expects financial institutions, as part of their evaluation, to implement any modification to their information security procedures and controls that appear to be necessary or appropriate in light of the risks associated with Internet-based services.”

Summary

In summary, the regulation of e-commerce in the financial services industry should be focused on the following principal objectives:

- International co-operation in on-line regulatory requirements should become a primary objective for international regulators who should strive for common standards and approaches at a global level.
- The challenge of IT competence should be left to the industry to manage but this does not mean that regulators should abdicate responsibility for the outcome.
- Further resources should be channelled towards building on existing consumer education initiatives.
- A full ‘audit’ of existing rules and regulations should be undertaken with amendments and guidance provided where required. The areas should cover, but not necessarily be limited to those identified above.
- Initiatives in the use of technology to improve existing regulatory processes should be pursued in ongoing consultation with the industry.
- Resources should be devoted to addressing new regulatory rule issues arising out of e-business and to providing the industry with certainty in terms of interpretation.

The ball is in your court – the challenge to management

In the last section we highlighted how regulators need to react to innovation within the Financial Services industry and the changing market infrastructure. We identified a number of areas where regulatory action is required in order to bring regulatory certainty to on-line activity and/or to address new regulatory challenges. However, this is a two-way street and there is plenty that the industry should be doing as well.

In this section, we look at the results of our research. We propose specific action that the management of a financial services e-business should be considering. As the leaders of the new economy, it is now the industry's chance to make a difference by:

- Ensuring competent management
- Playing its part in developing best market practice
- Taking the initiative in lobbying governments/regulators in situations where they are restricting the ability to develop e-business opportunities

The establishment of best practice in industry will prevent regulators having to regulate in a prescriptive manner.

So, what should management actually be doing? Our view is that to deal with these emerging threats effectively, financial institutions need, as a minimum, to have:

- A strategic approach to information security, building best practice security controls into systems and networks as they are developed
- A proactive approach to information security, involving active testing of system security controls (e.g. penetration testing), rapid response to new threats and vulnerabilities and regular review of marketplace developments
- Sufficient staff with information security expertise
- Active use of system-based security management and monitoring tools
- Strong business information security controls

In the section 'Key messages for e-managers and regulators', we identified some key action points for senior management and in this section we explore, in greater detail, some of the issues underlying these points.

It is the general responsibility of the CEO/directors of a financial services e-business to manage the activities of technical innovators and entrepreneurs in the business. They should ensure that the newly delivered on-line business has the benefit of prudent management and supporting infrastructure.

Fundamentally, a business needs to possess the necessary knowledge and skill to manage; hence the directors should review and challenge the composition of the board on a regular basis to ensure the correct skills exist to effectively manage new products and businesses.

It is essential that the board of directors and senior management gain an appropriate oversight by implementing a comprehensive technology risk management process. As the Internet Banking Comptroller's Handbook identified, the three basic elements of risk management of new technologies are:

- The planning process for the use of technology
- Implementation of the technology
- The means to measure and monitor risks

Planning

Traditionally, the role of the board and senior executives in a financial services company has been to monitor the organisation's exposure to business risks such as market and credit risk and to safeguard the future of the organisation. Computer systems and their successful implementation have always been an important element of good governance, though typically the risks associated with computer systems have not enjoyed the same priority on the board agenda as business-related risks.

Getting the organisation's strategy right is currently focused on the manner in which technology is used to enhance the position of the business. There are many reasons why technology is so important; for example, it offers:

- The chance to access a far greater number of customers or investors than face-to-face or telephone communications could ever hope to achieve
- A very cost-effective means for transacting business
- The potential for horizontal and vertical integration of product and service offerings
- Lower barriers to entry for new market competitors
- A threat of disintermediation for those whose services offer little added value

Clearly getting the strategy wrong or not having a strategy which takes into account the new paradigm represents a serious threat to the survival of an organisation. Indeed we have seen examples where the stock value of established organisations with strong market presence has been adversely affected by failure or non-existence of an e-business strategy.

This raises the question whether or not senior management in old economy organisations have the technological understanding to take advantage of the opportunities offered by the new economy approach to business. Conversely, the lowering of barriers to entry to many traditional markets and the explosion of new organisations seeking to carve out a marketshare, challenge whether or not the skills of managers in new economy organisations are adequate. These new organisations with their strong bias towards technology may lack the management capability to successfully address more traditional business risks such as market and credit risk.

Consequently, the challenge facing senior management across the whole spectrum of financial services is all the more significant. The value of seeking external advice and assistance is today of paramount importance for most organisations as it is unlikely that they will all have the potential to leverage the skills of the existing employee base.

Implementation

Assuming a credible business strategy has been identified, the next challenge is its implementation. Whilst it is today almost impossible to achieve 'first mover advantage' in many fields of financial services, there remains the need to minimise time to market of products and services. For example, an established business runs the risk of haemorrhaging customers to new market entrants or a more nimble competitor if their own products and services do not meet the demands of the market.

The implementation of new systems has never been a risk-free exercise. There is no shortage of anecdotes about IT projects that were late, over budget or error prone or failed to meet performance objectives. This is not a new phenomenon; so why should we expect implementation of e-business solutions to be any different?

It is important that every effort is made to mitigate the risks associated with systems implementation conducted in short time frames. Development approaches must be optimised and testing conducted to a

level which affords comfort that the systems will stand up to the rigours and demands placed on them in an operational environment. Risk mitigation must be allied to informed and calculated risk-taking in order to deliver solutions that are fit for purpose in the shortest possible time frames.

In addition to robust systems, there must also be an equally robust operational environment – in an ‘e-enabled’ world if the system is unavailable, the organisation is effectively closed for business. Consequently, it is important that there is adequate investment in maintaining system security, capacity and operational resilience.

Measuring and monitoring risks

In order to identify, measure, monitor and control risks associated with new technologies effectively, the IT department plays an important part as do senior management who oversee the operation.

The IT director should be responsible for setting high standards in IT capability and effectively implementing these through a process of self-regulation. In addition, the board may wish to integrate the role of the IT department into the firm’s regulatory and compliance control procedures, as IT has a key part to play in delivering compliant services and satisfying regulatory requirements in the new e-commerce environment.

To monitor risks, the IT department should develop system testing and surveillance methods to manage and control operational risks. At the same time, the compliance department should ensure that monitoring and control processes are keeping pace with innovation, and are effective in supporting front office delivery.

A monitoring system, accompanied by regular reports covering systems performance, should be devised. This will increase the board and senior management’s ability to monitor and manage various risks.

The board and senior management should consider appointing an internal/external auditing function to provide an important independent control mechanism for detecting and minimising risks. The role of an auditor is to ensure that appropriate standards, policies, and procedures are developed, and that the institution consistently adheres to them.

With the growing trend in outsourcing services in middle and back office functions, management should design appropriate controls over the outsourced activity service provider if they decide to place reliance on third parties. They should ensure there is an appropriate oversight programme in place to monitor the provider’s controls, condition and performance. The institution can thereby ensure security, reliability and integrity are not compromised.

To limit risk of disruptions in internal processes or in service or product delivery or unauthorised intrusions, the management must develop contingency plans that establish its course of action in the event of a system disruption. Such contingency plans should be as secure as their production operations. This will limit the institution’s exposure to reputation damage risk. This is also important in cases where services are outsourced.

Furthermore, senior management should take responsibility for shaping the regulatory approach to the regulation of e-commerce activity through lobbying and consultation processes. Regulators are looking to the industry to participate in the debate and this creates unprecedented opportunities to affect the development of policy, and enormous risk if the industry’s constituents remain on the sideline.

About PricewaterhouseCoopers

Regulatory

PricewaterhouseCoopers is the leading global provider of regulatory consulting and advisory services in the financial services sector. Our international network, comprising offices in 150 countries, enables us to offer a truly global regulatory advisory service.

Our dedicated Financial Services Regulatory Consulting and Advisory specialist teams offer proactive regulatory advice to regulated firms and other financial institutions around the world.

The teams, comprising over 500 people around the world, have extensive knowledge and experience of regulatory rules, codes of conduct and prudential supervision. The teams blend the experience of former senior regulators and compliance managers with assurance skills. This depth of expertise means we are well placed to:

- Explain how detailed regulatory requirements need to be applied
- Advise regulatory agencies on ways of enhancing their regulatory and supervisory regimes, including assisting in investigative and enforcement actions
- Assist in implementation of new requirements, such as responsibilities for senior managers
- Identify and help manage regulatory risks and compliance issues, in particular risks:
 - In periods of change
 - Associated with new products or distribution channels
- Work with management to establish or review the effectiveness of compliance policies, structures, controls and processes to manage the risks for better business, including advising on the use of technology to maximise the effectiveness of monitoring and minimise costs
- Advise on how to manage regulators' expectations properly and build relationships based on mutual trust

E-consulting

Managing risk and compliance issues requires an extensive set of technical and business skills. PricewaterhouseCoopers brings this varied skill set to engagements. Our capabilities include strategic risk management, security and control engineering, operational risk assessment and trusted third party and TriStrata solutions.

We have worked extensively with many of the world's leading financial services companies to deliver not only risk and compliance solutions but also support across a whole range of e-commerce and e-business issues. In doing so we make frequent use of our proprietary e-Business Maturity Model Assessment Tool, emm@™.

We use emm@™ to help companies understand their current e-business capabilities and chart their e-business future.

The model defines five levels of maturity in a successful e-business that enable a company to benchmark their e-business characteristics against best practices. The emm@™ model's world-wide best practices address one business aspect at a time, enabling a company to:

- Facilitate e-business planning and identify additional opportunities
- Maximise operational efficiency
- Manage e-business related risks

Appendix 1 – To be in (e-)business tomorrow, what should financial services companies be doing today?

Tomorrow's leading financial services organisation will certainly have a significant stake in e-business whether this is on a business-to-business or business-to-consumer basis. The question, therefore, arises, 'what does the organisation of today need to do to help position themselves to be tomorrow's leader?'

Accepted wisdom is that to succeed in the information age, businesses must build trust as this increases confidence, reduces inhibitions and barriers and hence allows people to transact business more freely. If it is for each organisation to implement the appropriate infrastructure to enable trust to be established, it is for the regulators to establish the policies which will ensure that that trust is not abused. Consequently, regulatory reform is likely to revolve around the following:

- Striving for excellence in IT to ensure high availability of services.
- Utilising the technology to improve compliance monitoring processes.
- Protecting confidence in the markets and achieving confidence in the security and reliability of electronic delivery systems. This is essential if, for example, electronic signatures are to become the norm for conducting business. Given the potential for cost saving and improvements in efficiency, these developments are inevitable once the legal framework for recognising digital signatures is in place.
- Identifying any additional issues that authorised firms should address from a commercial and regulatory perspective:
 - Record keeping requirements
 - Procedures for handling electronic mail
 - Review of internal controls and procedures with a focus on data security and business continuity

Regulators, generally, have adopted a policy of technological neutrality, that is they seek to apply existing rules and policies regardless of the medium. The basic principle underpinning financial services regulation is that firms are competent, that is that they are capable of managing their businesses. However, where a firm is providing services over the Internet, regulators are increasingly seeking satisfaction that the firm is managing risks properly. It is vital, therefore, that the financial services industry sets itself high standards in IT capability and effectively implements them; this should be achieved through self-regulation rather than any direct 'interference' from the regulators themselves.

Meeting obligations to customers is not easy, as the following examples illustrate:

- 90% of web site businesses have suffered significant operational problems.
- E-Bay (on-line auction house) stocks dropped by 18% in one day after a 22 hour outage.
- In the UK, Egg's systems collapsed just three days after launch of the credit card.
- Also in the UK, Halifax had to close on-line share dealing for a day as a result of processing errors in its software.
- In the US, eToys failed to deliver in time for Christmas '99.

Maximising the opportunities offered by the Internet demands a coherent and well thought out response. This response needs to include many, if not all, of the following areas.

Discussing and agreeing strategy

The key risks in conducting financial transactions in an e-commerce environment include:

- | | |
|--|---|
| Denial of service, vandalism and sabotage on the Internet | <ul style="list-style-type: none">• Services cannot be used as a result of being compromised and maliciously damaged by another party, generally a hacker. |
| Breach of privacy or customer confidentiality | <ul style="list-style-type: none">• Transactions are not sufficiently protected and message integrity and confidentiality could be intercepted. |
| Theft and fraud on the Internet | <ul style="list-style-type: none">• Services appear to be genuine but are a front with the intention to collect funds through fraudulent means. |
| Violations and data integrity attacks | <ul style="list-style-type: none">• Transactions are intercepted, data is compromised and transactions may be altered without detection. |
| Security | <ul style="list-style-type: none">• The configuration of the network for remote connections is not thoroughly protected.• Event recording is not sufficient to record all activity.• Internal security, both logical configuration and physical location of sensitive data, does not maintain an acceptable level of integrity and confidentiality. |

E-commerce providers, therefore, need to devise and implement strategies that address these risks. Such plans need to recognise the following three stage process, which we discuss in greater detail below:

- Establishing trust
- Ensuring security
- Delivering operational governance

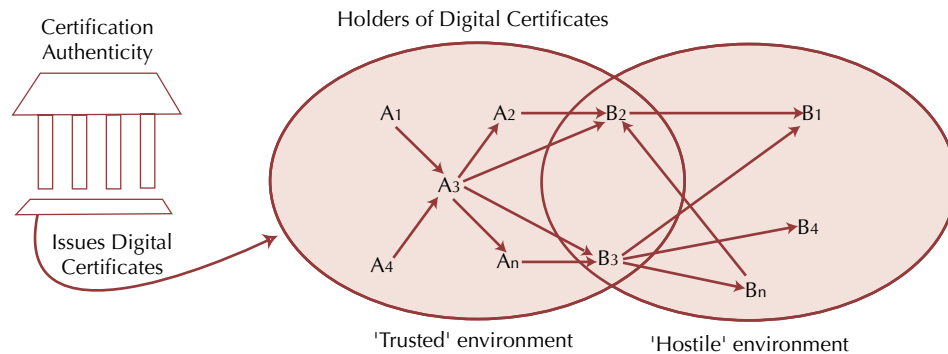
Establishing trust

Establishing a level of trust can be achieved on an enterprise level with distributed control either centralised or dispersed between each business area, or through the use of a third-party trust service. The foundations upon which trusted third parties operate are the policies and practices which establish the standards for conducting business and the mechanisms for providing high levels of assurance and accountability. These include:

- **Policies** that establish a legal infrastructure for the digital certification process. These should be contained in a published document, available for public review.
- **Controls** are important because they ensure that policies are being implemented as intended, and in a consistent manner.
- **Liability** assumption is a requirement to help assure customers that their digital assets will be diligently protected.
- **Auditability** is an important attribute because it signifies commitment to its business and serving global customers.

Third-party trust refers to a situation in which two or more entities are able to exchange information (data) in a secure environment knowing that they can be confident in the origin and destination of all

transmissions. The role of the trusted third party is to issue certificates to entities wishing to exchange data such that each certificate holder is a legitimate recipient or source of data. At a high level, this is illustrated in the following diagram.



A-type organisations exchange digitally signed messages and can 'trust' the integrity and origin of those messages.

B-type organisations exchange messages but because they are not members of the digitally certificated community they cannot necessarily 'trust' the integrity and origin of those messages.

There are also a number of other elements recognised as being critical to the development of trust, for example:

- Disclosing business practices
- Introducing business processes robust enough to meet your obligations
- Including 'seals of approval' on the web site
- Posting an independent audit opinion on the web site.

Ensuring security

In essence, the security requirements of any e-commerce service are to prevent unauthorised:

- Modification of information (integrity)
- Disclosure of information (confidentiality)
- Withholding of information or resource (availability)

An operational risk management checklist for ensuring security should cover the following items as a minimum:

- 1 Defining a security policy.
- 2 Defining a privacy statement.
- 3 Ensuring the availability of servers, including maintaining regular backups during the day so that recovery can be achieved up to and including the last processed transaction.
- 4 Recording all access and transactions to ensure auditability.
- 5 Supplying 'Smartcards' for authentication purposes.
- 6 Developing and managing a Certificate Policy for Public Key Infrastructure (PKI).
- 7 Dependant on the trust model applied, establishing a Certification Authority (CA) and Registration Authority (RA):
 - The CA will be responsible for digitally signing certificates in a trusted infrastructure, binding a user or function to a public key, as defined in the Certificate Policy, and for the distribution of Certificate Revocation Lists.
 - The RA will be controlled from within another department and is responsible for validating the identify of the user, providing authentication mechanisms and key and certificate management, including the management of certificate revocation requests.
- 8 Maintaining a 24 hour help desk with facilities for different spoken languages.

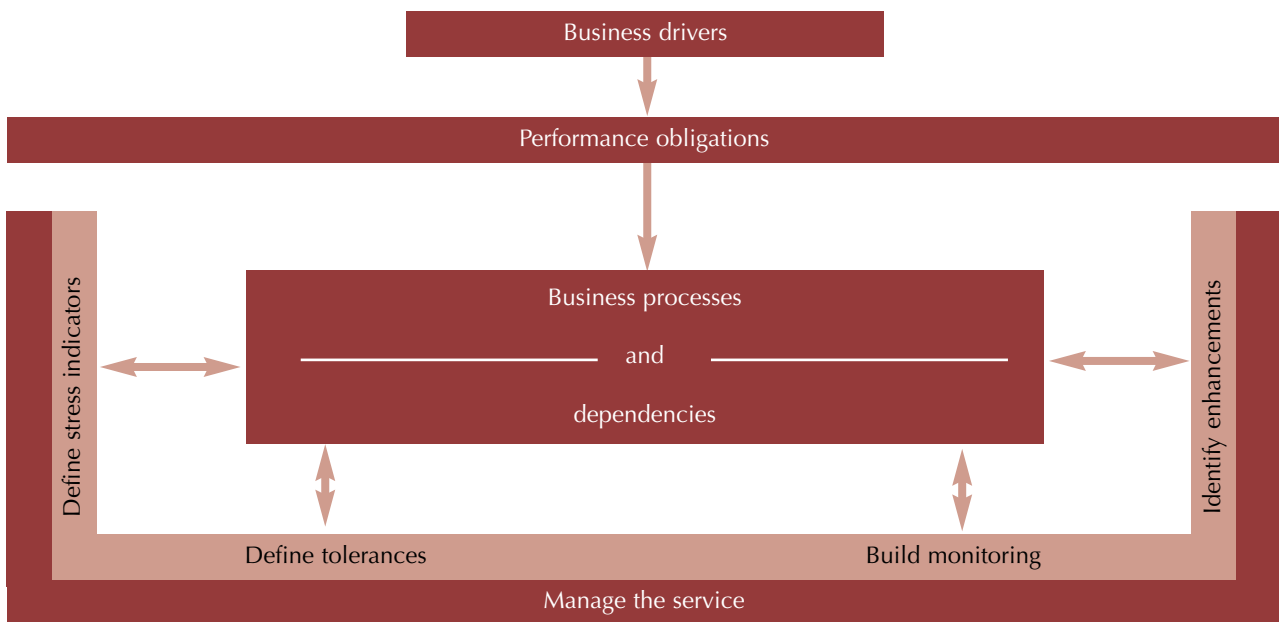
Delivering operational governance

To ensure that the appropriate services are available to support the activity when operational, companies need to address the risks, controls and procedures relating to the following:

- Authentication
- Authorisation
- Non-repudiation (including secure time-stamping)
- Auditability
- Availability
- Privilege management
- Third-party management

Establishing robust processes to meet obligations

The following diagram depicts the relationship between business drivers and organisation's operational performance objectives. The concept is quite simple in that metrics are defined for monitoring the performance of the business processes providing the basis for efficient management of the service. The metrics should be driven by the needs of the business.



Investing in technology/upgrading systems

Minimum standards for engaging in e-commerce:

- Internet banking
 - The message standard Open Financial Exchange (OFX) was created through a consortium consisting of Microsoft, Intuit and Checkfree in 1998 to provide consistency for payments.
 - Integriion's Gold Message Standard was created from a consortium consisting of IBM and 16 banks in the USA, with the purpose of providing a similar offering to OFX but with greater inter-operability between banking systems.
- Mobile phone banking – with SIM card supporting a recognised encryption standard – the Wireless Application Protocol (WAP), initiated by Ericsson, Motorola, Nokia and Unwired Planet, has been created to provide a means to access a variety of wireless technologies including GSM, CDMA and PHS.

Appendix 2 – Key global regulatory releases and publications

This is not an exhaustive list but is illustrative of the guidance and releases issued by regulatory authorities and others around the world. Many of these have been referred to in the compilation of this study.

US

- 'From Wall Street to Web Street: A Report on the Problems and Promise of the On-line Brokerage Industry', Office of New York State Attorney General Eliot Spitzer, prepared by Investor Protection and Securities Bureau and Internet Bureau (22 November, 1999)
- FRB: SR 00-4 (SUP) 'Outsourcing of Information and Transaction Processing', by the Division of Banking Supervision and Regulation of Board of Governors of the Federal Reserve System, 29 February 2000
- 'Internet Banking: Comptroller's Handbook' (October 1999)
- Testimony of James D. Kamihachi (25 March, 1999)
- News release by OCC – NR 2000 – 11
- 'Special Studies on Technology and Banking' (Karen Furst et al)
- 'OCC Bulletin 98-38: Technology Risk Management: PC Banking', Comptroller of Currency Administrator of National Banks (24 August, 1998)
- 'OCC Bulletin 98 –31: Guidance on Electronic Financial Services and Consumer Compliance', Comptroller of Currency Administrator of National Banks (20 July, 1998)
- OCC Bulletin 99-20:
- The Forrester Report – Regulating Global e-Commerce
- Testimony of James D. Kamihachi (25 March 1999)
- Speech by William J McDonough (6 April 2000)
- 'Bank Regulation on Cyberspace' (P.A.Schott, PricewaterhouseCoopers)
- 'Regulating on Internet Time', Remarks by Commissioner Laura S. Unger, US Securities & Exchange Commission, at Conference on Integrating Technological Advances for On-line Brokerages, New York, New York (22 September 1999)
- Empowering Investors in an Electronic Age, Remarks by Commissioner Laura S. Unger, US Securities & Exchange Commission, at IOSCO Annual Conference Sydney, Australia (May 17,2000)

Europe

- Securities and Futures Authority (UK) Board Notice 543
- 'Guidelines concerning the use of Internet by listed companies on a regulated market when they disseminate financial information', Commission des Opérations de Bourse, 3 May 1999
- 'Guidelines concerning the promotion or the selling of collective investment schemes mandated portfolio management services through Internet', Commission des Opérations de Bourse, 3 September 1999
- Decision 99-07 'Requirements and recommendations for investment service providers offering order reception-transmission or execution services involving reception of orders via Internet', Conseil des Marchés Financiers, 15 September 1999
- Swedish regulatory authority (Finansinspektionen) report entitled '2000:3 Internet and Financial Services', April 2000
- IMRO (UK) notice, 'The Internet' – May 1997
- PIA (UK) Regulatory Update 37 (August 1997), 'PIA and the Internet'
- SFA (UK) Board Notice 416, 'The Internet'

- SFA (UK) Board Notice 543 (7 April 2000), 'The Internet and electronic commerce'
- FSA (UK) Guidance release 2/98, 'Treatment of material on overseas Internet World Wide Web sites accessible in the UK but not intended for investors in the UK'
- FSA Guide to Banking Supervisory Policy (29 June 1998 – updated to 30 June 1999), 'Internet Banking'
- Deutsch Bundesbank Monthly Report – June 1999 – 'Recent Developments in Electronic Money'
- Bundesaufsichtsamt für das Kreditwesen (BAKred) – 'Marketing of Foreign Collective Investment Schemes on the Internet', 2 June 1998.
- Bundesaufsichtsamt für den Wertpapiererhandel Announcement, September 1999. 'Internet offers require a prospectus'
- Bundesaufsichtsamt für den Wertpapiererhandel Letter, February 2000: 'BaWe Reminds on-line Banks of Organisational Requirements'
- Securities Board of The Netherlands, Policy Document 99-0003 'Concerning the Internet in Relation to the Supervision of Securities Trading in The Netherlands'

Asia-Pacific

Australia

- Policy Statement 107, 'Electronic Prospectuses', published by Australian Securities and Investment Commission (ASIC)
- Policy Statement 118, 'Investment advisory services: media, computer software and Internet advice', published by ASIC
- Policy Statement 141, 'Offers of securities on the Internet', published by ASIC
- Policy Statement 150: 'Electronic applications and dealer personalised applications', published by ASIC
- Policy Statement 152: 'Lodgement of disclosure documents', published by ASIC
- Second Draft Expanded EFT Code of Practice and Commentary, by ASIC's EFT Working Group, January 1999
- Discussion paper on an expanded EFT Code of Conduct, by ASIC's EFT Working Group, 26 July 1999
- 'The On-line Corporation: Electronic corporate communications discussion paper', written by Elizabeth Boros, December 1999
- 'Multimedia prospectuses and other offer documents Issues Paper', written by Dr Elizabeth Boros, Centre for Corporation Law and Securities Regulation, The University of Melbourne and ASIC, December 1999
- RGECC (Research Group on the Law Enforcement Implications of Electronic Commerce) reports:
 - Issues Papers Series No.1 (Volume 1)
 - 'Contributions To Electronic Commerce' (Volume 2)
 - Research and Technical Advice (Volume 3)
- APRA's Policy Reform Program, Policy Information Paper, March 2000, Australian Prudential Regulation Authority (APRA)

Hong Kong

- Guidelines published by Hong Kong Monetary Authority (HKMA) to date:
 - Guideline No 15.1 Electronic banking, July 1997
 - Guideline No. 15.1.1 Security of Banking Transactions over the Internet, November 1997
 - Guideline No 15.2 Basel Committee on Banking Supervision's Paper on 'Risk Management for Electronic Banking and Electronic Money Activities, April 1998
 - Guideline No 15.3 Public Key Infrastructure and Legal Environment for Development of Internet Banking, October 1998
 - Authorisation of Virtual Banks, May 2000
- Guidelines published by the Securities and Futures Commission: Guidance Note on Internet Regulation, March 1999

Singapore

- Monetary Authority of Singapore (MAS) Circular FSG 02/2000 - 'Posting of Financial'
- MAS, Ministry of Finance and Registrar of Companies and Businesses – 'Guidelines on Offers of Shares, Debentures and Unit Trusts Through the Internet', 14 February 2000

Japan

- 'Japanese Big Bang (January 2000)' press release on Ministry of Finance web site [<http://www.mof.go.jp/>]
- 'Developments in the Regulatory Framework for Electronic Commerce in Financial Services', The Study Group Concerning Supervisory Administration of Electronic Commerce, Etc. in Financial Services (April 18, 2000)

Global Organisations

International Organisation of Securities Commissions (IOSCO)

- 'Bulletin Regarding Investor Protection in the New Economy' (May 2000)
- 'Securities Activity on the Internet Report' by Technical Committee (September 1998)

Organisation for Economic Co-operation and Development (OECD)

- OECD Ministerial Conference 'A Borderless World: Realising the Potential of Global Electronic Commerce'
- 'The OECD Action Plan for Electronic Commerce'
- 'Report on International and Regional Bodies: Activities and Initiatives in Electronic Commerce'
- 'Global Action Plan for Electronic Commerce prepared by Business with Recommendations for Government'
- 'Conference Conclusions'

The Forum of European Securities Commissions (FESCO)

- Press Release 22 December 1999 – 'FESCO announces a significant step forward for a common regulation of the European single market for financial services'
- Press Release July 7 1999 – 'Consultation Paper on Standards for Regulated Markets'
- 'Multilateral Memorandum of Understanding on the Exchange of Information and Surveillance of Securities Activities'

World Trade Organisation (WTO)

- 'Declaration on Global Electronic Commerce', adopted on 20 May 1998

Basel Committee

- Basel Committee on Banking Supervision (March 1998)

Appendix 3 – XML/XFRML languages

XML (extensible mark-up language) is one of a new generation of languages for the Internet. It is a universal system of tags that enables the content of a cell to be specified, be it text or numerical. Data formatted in XML and made available on the server can be made accessible to all applications.

This simple idea seems likely to spark off a revolution in information sharing between businesses and consumers as the full potential of a common data format is realised. With relatively small changes to existing systems, a company would be able to share data, in 'real time', with any other user of XML, who can then reformat the information to be used as desired. An example of the use of XML is FpML (Financial Products Mark-up Language) that a number of banks, led by JP Morgan, are developing to be able to exchange common data about a wide range of financial products, such as interest rate swaps.

Due to the simplicity of the language, relatively junior staff in any organisation can write programmes that present or check data in a certain format. One company already uses the language for invoicing suppliers over the Internet. Therefore, no invoices need be sent and delivery is almost immediate.

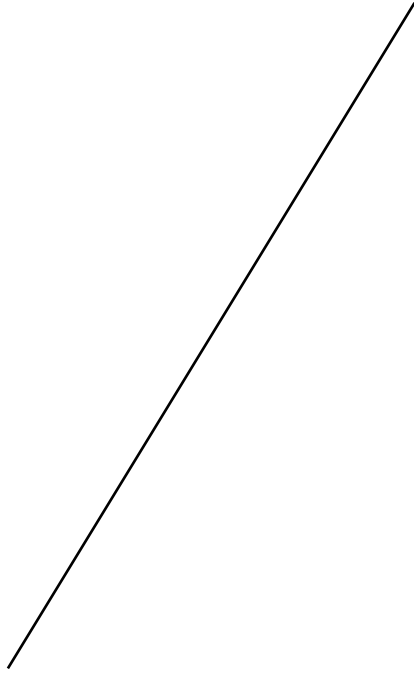
XML based derivatives are being developed with increasing speed. In the UK, we understand that XML has been used as the basis to enable electronic filing of tax, PAYE and VAT returns. Elsewhere, a group led by the US AICPA (certified accountants) is specifying XBRL (Extensible Business Reporting Language) another XML derivative, that is being developed for financial and non-financial corporate reporting.

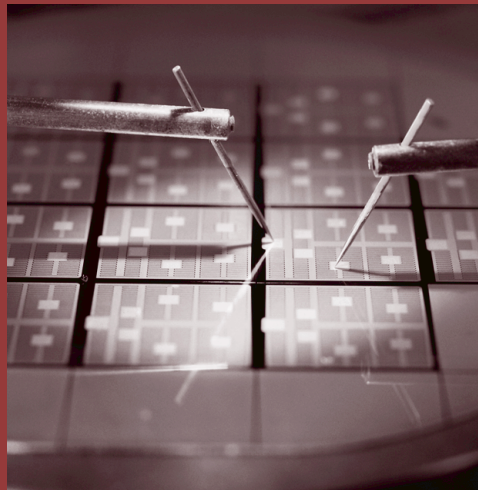
Whilst such initiatives are led by the need to communicate data externally, many are also looking at XML-based derivatives for internal systems as well. One clear advantage would be that all internal systems would operate on a web-friendly basis and thus reduce barriers to communications between entities that use individual systems to suit their own business activities or business/territorial environments.

Contact details

To discuss the implications for the various sectors, please contact your usual PricewaterhouseCoopers contact or one of the following people at the e-mail addresses listed or visit the e-business web-site www.ebusinessisbusiness.com.

PricewaterhouseCoopers Regulatory contact		
North America		
USA	Bob Bench, Roger Coffin David Albright John Campbell	bob.bench@us.pwcglobal.com roger.coffin@us.pwcglobal.com david.albright@us.pwcglobal.com john.campbell@us.pwcglobal.com
Canada	Lee Puschaver	lee.puschaver@ca.pwcglobal.com
Europe		
UK	John Tattersall	john.tattersall@uk.pwcglobal.com
Germany	Rolf Friedhofen	rolf.friedhofen@de.pwcglobal.com
France	Guy Flury	guy.flury@fr.pwcglobal.com
Belgium	Marc Vandemeuelbroeke	marc.vandemeuelbroeke@bg.pwcglobal.com
Holland	Wietse de Jong	wietse.de.jong@nl.pwcglobal.com
Switzerland	Pascal Portmann	pascal.portmann@ch.pwcglobal.com
Pan-European	Charles Ilako	charles.ilako@uk.pwcglobal.com
Asia-Pacific		
Australia	Jan Muysken	jan.muysken@au.pwcglobal.com
Japan	George E Stylianides	george.stylianides@jp.pwcglobal.com
Hong Kong	Rick Heathcote	rick.heathcote@hk.pwcglobal.com
Singapore	Dominic Nixon	dominic.nixon@sg.pwcglobal.com





PricewaterhouseCoopers (www.pwcglobal.com), the world's largest professional services organisation, helps its clients build value, manage risk and improve their performance. Drawing on the talents of more than 150,000 people in 150 countries, PricewaterhouseCoopers provides a full range of business advisory services to leading global, national and local companies and to public institutions.

These services include audit, accounting and tax advice; management, information technology and human resource consulting; financial advisory services including mergers & acquisitions, business recovery, project finance and litigation support; business process outsourcing services; and legal services through a global network of affiliated law firms.

PricewaterhouseCoopers refers to the member firms of the worldwide PricewaterhouseCoopers organisation.

e-business microsite address - www.ebusinessisbusiness.com

Copyright©2000 PricewaterhouseCoopers. All rights reserved. PricewaterhouseCoopers is authorised by the Institute of Chartered Accountants in England and Wales to carry on investment business. Designed by The Studio (11266 07/00).

Your worlds



Our people