The Internet & Financial Services: a CSFI report
Centre for the Study of
Financial Innovation

The CSFI was set up in early 1993 as a forum for new thinking about the international financial system. It is a charity, and is supported by approximately three dozen financial institutions—including clearing and investment banks, consultancy and accounting groups, and agencies like the Bank of England, the Treasury and the DTI. The CSFI is non-ideological; it advocates no political point of view beyond a belief in free and efficient markets.

The Chairman of the CSFI’s Trustees is Minos Zombanakis. The chairman of the Governing Council is Sir George Blunden. Other members of the Council include:

- David Bell, Pearson plc;
- Robert Bench, Price Waterhouse;
- Peter Birch, Abbey National plc;
- Peter Cooke, Price Waterhouse;
- Prof. Charles Goodhart, London School of Economics;
- John Heimann, Merrill Lynch;
- Henry Kaufman, Henry Kaufman & Co.;
- John Langton, ISMA;
- Sir Kit McMahon;
- Sir Peter Middleton, BZW;
- Sir Brian Pearse, LucasVarity and
- Sir William Ryrie, ING Barings.

The Chairman of the Centre’s Advisory Council is John Plender. The Director is Andrew Hilton, and the Co-director is David Lascelles.
Acknowledgements

This report is the product of eight working groups, comprising over 120 people from more than 70 institutions, which met under CSFI auspices in the latter part of 1996. The members of the working groups are indicated at the beginning of each chapter. The Centre is grateful to everyone who participated, and especially to those institutions which made their facilities available for working group meetings.

The final report was edited by David Lascelles, co-director of the CSFI (and formerly natural resources editor at the Financial Times). He was assisted by Andrew Hilton, director of the Centre, and by Davide Ferrara, director of studies. Among the CSFI staff who did background work for the report, special mention should be made of Benjamin Meth, Scott Vogel and Michael Smotryaev.

While every reasonable effort was taken by the CSFI to ensure that the submissions by the working groups were correct at the time of writing, no assurance or representation is given that the facts contained herein or opinions expressed are necessarily accurate or complete, nor that the report is in any way exhaustive or objective. Readers are strongly urged to seek additional independent advice before taking business decisions or other actions relating to the Internet, and not to do so based on this report. No responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication can be accepted by the authors, editors or publisher.
Andrew Winckler and I are very pleased to have been asked to write the foreword to this CSFI Report. The Report is a valuable contribution to the debate about how global electronic commerce will develop. The Working Parties are to be congratulated on the concise nature of their reports and the practical approach they have adopted in analysing the issues.

The CSFI has brought together a wide cross-section of the financial services community and provided a valuable forum for debate about the market structure, commercial and regulatory issues involved. Internet developments impinge on the whole range of the SIB’s functions and objectives. The Internet has the potential to alter the structure of markets and the traditional nature of the relationships between institutions, firms and their customers. In particular, I would like to concentrate on two related issues which go to the heart of regulation of the retail, rather than the professional, market.

The first is the way in which the Internet has the potential to strengthen the position of investors significantly. The very nature of the Internet allows the delivery of vast amounts of information, cheaply, to anywhere in the world. In future, access may well move from a relatively limited PC population to a larger, and far more diverse, TV audience. We may then see the incidence of retail usage growing hugely.

The Internet can, in some circumstances, provide the investor with the ability to search for investments and to analyse for him or herself performance and returns before taking an informed view about which to purchase. It may also be possible to buy that product or service on-line. This itself raises a number of interesting issues related to the technology. Will it mean a rethink as to the nature and level of regulation if the Internet can deliver a more educated investor and thus redress the “knowledge balance” between those offering financial services and the potential investor? Could the Internet be the vehicle which makes a “caveat emptor” approach to regulation more sustainable? In the future, will regulation be orientated towards the “authorisation” of software packages rather than people or firms? Clearly there are a number of issues, which are identified in this Report, that need to be resolved (eg timely distribution of information; digital signatures; security of transactions) but the prospect of a significant shift in regulation remains a possibility.

The second important issue the Report highlights is that the existing regulatory framework throughout the world is, essentially, based on the application of local laws to those wishing to provide the physical delivery of financial services to different jurisdictions. The Internet offers the prospect of a global market and it does so on the basis of relatively inexpensive access for the provider and the customer. Investors throughout the world will be more cost effectively
The Internet and Financial Services

accessible via the Internet than through any other medium. This means that whilst the Internet does not necessarily raise any fundamentally new jurisdictional issues, the sheer force of the combination of its attributes may have the power to shift the point of focus of regulation. Concepts of “local” regulation may quickly become out-moded, as may the notion of a service being provided from one place. The movement towards a global marketplace would logically point to a movement to global regulation. Whether, or how quickly, this might happen is not clear.

There are two broad options facing regulators around the world. Regulators could attempt to maintain local jurisdictional control by, for instance, imposing regulatory requirements which force firms to limit access to their sites. Given the structure of the Internet, such requirements could be difficult for companies to comply with effectively and for regulators to enforce. Alternatively, regulators could move to a position where there were mutually agreed and recognised standards of regulation which allowed financial services firms to offer services in any other jurisdiction as long as they were appropriately authorised to carry on that business in the jurisdiction in which they were authorised.

This, in my view, is going to become the central debate in years to come. Global regulatory frameworks may be some way off, but the CSFI Report is a timely reminder that these issues are not purely of academic interest but are fast becoming “real world” issues.

Sir Andrew Large
Chairman
The Securities and Investments Board

In the UK there are many practical issues about how existing regulation affects the way in which firms can use the Internet now and how investors should view financial services offered over the Internet. The SIB has taken several initiatives in these areas. We organised an inter-regulatory meeting in February of this year to take stock of the use of the Internet currently being made by the industry. Also in February, the SIB established its own Internet site (http://www.sib.co.uk) on which a wide range of regulatory information is available including a number of “Investor Alerts” and information about the implications of carrying on investment business over the Internet.

We know from our contacts with the industry that firms are also concerned about the implications of having a presence on the Internet in terms of their legal exposure in other jurisdictions in which their Internet site can be viewed. This is something which we are taking very seriously. We try to provide firms with our views about how the Act applies to material available in the UK and to make those views as widely available as possible. Many of the regulatory issues raised in this Report reflect questions already raised directly with the SIB by the industry. I see continuing dialogue with the financial services industry as vital, and it is an area into which we will be putting additional effort in the
coming months. In particular, the advertising provisions in the Act have raised specific concerns which we have in turn raised with the Treasury. We have also been engaged in a general awareness campaign (in the press; at conferences and through the Internet site) to explain the SIB’s views.

We have also been working closely with the Self Regulatory Organisations ("SROs"). In addition, we have had detailed discussions with the SROs about the need to clarify the application of their conduct of business rules and both IMRO and the SFA have now issued guidance — although this is by no means the final word on the matter given the speed of developments on the Internet and the need for regulatory approaches to be refined accordingly. The PIA is also addressing Internet issues as part of its “Evolution Project”.

Internationally, we have been making the case within the International Organisation of Securities Commissions ("IOSCO") for shorter term practical issues to be addressed. We are keen, for instance, that the merits of encrypted “regulatory kitemarks” for sites are fully explored, in addition to agreed disclaimers and warnings, to provide investors and firms with a degree of legal and regulatory certainty.

In spite of its potential, and benefits, there is no question that within the UK and internationally there is increasing recognition that the Internet poses real challenges which cannot be ignored. We now feel it is important to provide formal guidance about the impact of the Internet on the current regulatory framework, which we aim to issue before the end of the year. This will, amongst other things, confirm views the SIB has expressed in relation to specific issues that have been raised over the past 18 months relating to the applicability of various provisions in the Act to investment business over the Internet. It will also address the investor protection issues which have formed the basis of our discussions with the SROs regarding conduct of business rules.

As the Report points out, regulation provides both a potentially large stumbling block to the development of the Internet, given its various uncertainties, and at the same time an important safeguard which could allow its successful development as an investment marketplace. Regulation must play a positive role by providing an environment in which investors can operate with confidence and in relative safety. We are convinced that this challenge can be met, as indeed it must in view of the potential new opportunities the Internet provides for businesses and investors alike.

Andrew Winckler
Chief Executive
The Securities and Investments Board
In February 1996, the Centre organised a round-table discussion on the Internet and financial services, with four lead speakers – Joseph de Feo (Barclays), Paul Taylor (Financial Times), Andrew Boswell (ICL) and Steve Sim (BT). Having held several meetings on the impact of new technology on the financial sector, this seemed a logical development for the CSFI – but we did not expect the response we received.

Normally, CSFI round-tables attract an audience of 30-40 (indeed, we don’t want more than 45). This meeting, however, produced an audience of close to 200 – standing-room only at the National Liberal Club. It was clear that we had identified a real need: in the financial services sector, people (particularly managers) are hungry to know more about how this new phenomenon is going to affect their business.

Despite the best efforts of our speakers, the round-table was inevitably a bit of a zoo, and probably did not answer the key questions. But it was clear that there was real enthusiasm for the subject. We, therefore, decided that we would organise a series of follow-up meetings, built around the various areas that are likely to be most affected by the Web. Rather arbitrarily, we identified these as:

- retail banking;
- personal finance (including life assurance products);
- insurance and reinsurance;
- equity trading;
- regulation;
- payment and settlements;
- security; and
- crime.

For each of these areas, we identified a chairman, and invited participants from the original round-table (and other interested parties) to join one or more of the working groups. We ended up with around 120 participants from over 70 institutions.

Each of the groups met six to eight times in the latter part of last year, usually for a working lunch hosted by one of the institutions involved (for whose generosity we are grateful), and the result was a series of self-contained reports. These were then edited, expanded and generally tweaked about to produce the present volume. As noted elsewhere, there remain differences of
The Internet and Financial Services

interpretation among the contributions of the various groups; but, taken as a whole, they provide a comprehensive view of the Internet and financial services. Clearly, this subject is a moving target, and things will change. The CSFI, therefore, hopes to keep several of the groups going; but we believe that the present volume does cover the field as of mid-1997.

Andrew Hilton
Director, CSFI
Contents summary

Executive Summary 1

Section one: Overview 5

Section two: Key financial sectors 31
  • Chapter one: Retail banking ........................................ 31
  • Chapter two: Personal finance ..................................... 53
  • Chapter three: Insurance and reinsurance ....................... 73
  • Chapter four: Equity trading ...................................... 89

Section three: Internet drivers 105
  • Chapter one: Regulation ........................................... 105
  • Chapter two: Payment and settlement systems .................. 137
  • Chapter three: Security ............................................ 155
  • Chapter four: Crime ............................................... 177

Glossary 199

Index 211
## Contents

### Executive Summary

SECTION 1: OVERVIEW

- What is the Internet? ................................................................. 5
- The Internet today ................................................................. 7
  - The Internet: hard or hype? .................................................. 8
- Relevance of the Internet to financial services ....................... 9
- The technological impact ....................................................... 11
- What will drive the Internet? .................................................. 12
- Will the Internet gain acceptance for selling financial services? ... 15
- Present strategies ................................................................. 17
- Threats and opportunities ...................................................... 18
- Creating the conditions for Internet commerce ....................... 23
- Social issues ................................................................. 27
- Conclusions ................................................................. 28

SECTION 2: KEY FINANCIAL SECTORS .................................................. 31

Chapter 1: Retail Banking .................................................. 31

1. Introduction .............................................................................. 33
2. A step change for retail banks? ............................................. 34
3. What the Internet could mean for retail banking .................... 36
   - The process ........................................................................ 36
   - The functions ...................................................................... 38
     - Transaction balances .................................................. 38
     - Payments ...................................................................... 39
     - Deposits and loans .................................................. 40
     - Risk Management .................................................. 42
     - Information .................................................. 44
4. What is being done? ............................................................. 44
   - US ..................................................................... 45
   - Europe ..................................................................... 46
5. Where next? ..................................................................... 48
Chapter Two: Personal Finance

1. Introduction ................................................................. 55
2. Who uses the Internet? .................................................. 55
   • Regular users ......................................................... 56
   • Occasional users .................................................... 56
3. The financial services spectrum ...................................... 58
4. Setting up and managing a personal financial services Web site ... 58
5. Current offerings ........................................................ 61
6. How easy is it to navigate the Internet? ............................ 63
7. The effect on UK IFAs (and what they can do about it) .......... 69
8. The way ahead – how to make the system easier for the investor .... 71
   • How might consumers be encouraged to have greater confidence in the Internet? ......................... 71
9. Conclusion .................................................................. 72

Chapter Three: Insurance and Reinsurance ........................... 73

1. Introduction .................................................................. 75
2. Basic assumptions ....................................................... 75
3. Current state of Internet usage ....................................... 76
   • Perceptions of the Internet .......................................... 76
   • Deployment among UK general insurers ...................... 76
   • Internet developments ............................................... 78
   • Key issues for general insurers .................................... 80
   • Deployment by Lloyd’s agencies .................................. 80
   • Deployment among reinsurers ..................................... 82
   • Deployment by insurance and reinsurance brokers ........ 83
4. Impact of the Internet on general and reinsurance markets .... 84
   • Implications for general insurers ................................. 84
Contents

- The politics of encryption .................................................. 113
- Opportunities ................................................................. 113

5. Areas of regulation which affect use of the Internet ............... 115
  - Existing financial services legislation in the UK ................ 115
  - Existing bank regulation in the UK .................................. 120
  - EU regulation of financial services ................................. 121
  - US regulation ............................................................. 123

6. Data protection legislation and the Internet ......................... 124
  - UK data protection ...................................................... 124
  - The EU Directive on data protection ............................... 126

7. Other areas of regulatory concern .................................... 126
  - Contracting on-line ...................................................... 126
  - Money laundering ....................................................... 129
  - Duties of secrecy .......................................................... 129

8. Recommendations of the working group ............................ 130
  - Protection of genuinely “foreign” sites ........................... 130
  - Regulatory guidance on format of electronic documents ...... 132
  - Closer co-operation with regulators ............................... 133
  - Location of servers ..................................................... 134
  - Should the industry lobby on e-cash? .............................. 134
  - Data protection .......................................................... 134
  - Digital signatures ......................................................... 134
  - Contracting on-line ...................................................... 134
  - UK Web site management .............................................. 134

Chapter two: Payment and settlement systems ....................... 137

1. Introduction .................................................................... 139
  - Distinction between retail and wholesale payments .......... 139

2. Retail payment and settlement on the Internet ....................... 140
  - Credit, charge and debit cards ...................................... 140
  - Electronic cash and micropayments ................................ 143
  - Multi-currency payment systems ................................... 146

3. Wholesale payment and settlement systems ......................... 146
  - Back office and clearing support functions ...................... 147

4. New issues in payment and settlement systems
   arising from the Internet ................................................ 147
Chapter three: Security

1. Introduction .................................................. 157

2. Is Internet security a problem for financial institutions? .............. 157

3. Assessing the seriousness of the problem ........................................ 158
   • Risk = Vulnerability x Threat ........................................... 158
   • Specific business risk can usually be managed ..................... 159
   • General access via the Internet can pose a much greater risk .... 161

4. Solutions ........................................................................ 162
   • Cryptography ............................................................... 163
   • Financial transactions over the Internet can be secure .......... 168
   • Other forms of security ................................................. 169
   • Confidentiality as a problem ........................................... 171

5. Summary of risks and measures to address them ......................... 171

6. Business opportunities for financial institutions .......................... 172

7. Conclusions and recommendations ........................................... 175

Chapter four: Crime

1. Introduction ...................................................................... 179
   • Background ...................................................................... 179
   • Definitions ...................................................................... 179

2. Problem definition ................................................................ 180
   • Types of crime .................................................................. 180
   • Subversion of public infrastructure ................................... 181
   • Sex-related offences ...................................................... 182
Contents

- Fraud ................................................................. 182
- Hacking .................................................................. 183
- Software piracy .................................................. 183
- Contamination ....................................................... 184
- Victims of crime on the Internet ......................... 185
- Perpetrators of crime via the Internet .................. 186
- Scale of the problem ............................................. 188
- Contributing factors ............................................. 188

3. Problem analysis .................................................. 191

4. Response ............................................................. 192
   - International ..................................................... 192
   - Government ..................................................... 192
   - How secure is secure? .................................... 195
   - Security specialists ....................................... 196
   - Self-help ........................................................ 196

5. Conclusions and recommendations ...................... 198

Glossary ................................................................. 199

Other CSFI publications ......................................... 207

CSFI sponsors ......................................................... 209

Index ..................................................................... 211
EXECUTIVE SUMMARY

This report, the product of eight CSFI working groups which met in the latter part of 1996, considers the impact of the Internet on the financial services industry, particularly banking, personal finance, the equity markets, insurance, and payment and settlement systems.

In all these areas, the report concludes that the Internet has the potential (albeit, once a number of obstacles have been overcome) to bring about revolutionary change by transforming the way business is conducted, by providing a new means for delivering services, and by imposing a new set of economics on the finance industry, particularly on the retail side.

In this environment, some of the industry’s most familiar institutions could disappear and be replaced by a new generation of electronic service providers and screen-based markets, operating at much more competitive levels of service and pricing than exist today.

The Internet could do this by:

- stimulating more intense competition in the financial services market, e.g. by admitting new entrants, making pricing more transparent, and raising service expectations to new levels;
- tilting the market in favour of service suppliers with technology and marketing know-how, and against those with traditional skills and cost structures;
- “empowering” the customer by giving him direct access to market information and providing him with the means to execute his own deals; and
- removing geography as a constraint to the finance business (e.g. floor-based markets, bank branches, national preferences), and creating an industry that exists almost entirely in cyberspace.

Because the Internet would improve the convenience and reduce the cost of financial services, the main beneficiary of all these changes (if they took place) should be the consumer. In an Internet world, he would be able to roam through an electronic marketplace, seeking out the best services and prices, and managing his own financial affairs— even to the point of being able to run his own personal bank account.

From the service supplier’s point of view, the Internet could also open up new marketing possibilities, particularly for non-traditional suppliers who are unencumbered by earlier structures and attitudes. On the other hand, the Internet would undermine the ties of loyalty (or inertia) that have bound customers to financial institutions in the past. It could also cut out the middleman and force down prices. Existing financial service providers would therefore be vulnerable, especially:
The Internet and Financial Services

- those with inflexible legacy systems (e.g. clearing banks);
- those who profit from market opaqueness (e.g. life insurers); and
- those who live by intermediating between suppliers of services and end users (e.g. brokers).

The potential for change is great in each of the sectors covered by the report:

- **Banking**: The Internet could hasten the transition to screen-based home banking. The consumer would then be freed from ties to a single supplier and would be able to shop around for the best loan and deposit rates. Although this would undercut the banks' traditional role, it is possible that they could compensate by finding new business opportunities as guarantors of Internet commerce.

- **Personal finance**: The “empowerment” of the consumer could cut out the middleman and stimulate the market for “direct” mortgages, life insurance, investment services etc. On the other hand, the Internet has already sparked a proliferation of new services and sources of information which could create demand for specialist “info-mediaries” with high levels of Internet familiarity.

- **Equity markets**: The Internet will provide the investor with direct access to stock market prices, research and execution. This could further reduce demand for expensive full service broking, and focus competition in areas such as discount broking and the provision of screen-based stockbroking accounts. There could also be a market for fee-based investment advice and research over the Internet. Enthusiasts believe that equity markets will increasingly migrate to the Internet, possibly into a single, global non-stop market. The potential also exists for primary stock issues over the Internet by means of electronic prospectuses. The scope for change at the wholesale end is smaller, both because of security and reliability concerns, and because there already exist proprietary trading systems with much higher performance capabilities than the Internet. That said, the Internet may eventually provide a means for settling equity trades.

- **Insurance**: In general, the industry has been slow to adapt to electronic advance. However, proprietary systems and the Internet are currently both being developed to provide channels for information and transactions at both the wholesale and retail ends of the market. There is a belief that the elimination of geography will advantage remote markets like Bermuda; equally, however, it could bring new business to established markets whose reputation transcends geography.

While all the above is possible with the Internet technology that already exists, the report also expresses reservations about the pace at which delivery of financial services will evolve over the Internet. The potential is there; but it would be wrong to ignore the many problems that the Net faces in the financial services area:
Executive Summary

- Although the financial services sector sees the potential of the Net, and has established a substantial presence on it, other sectors are already ahead in using it to generate real business. Indeed, recent figures suggest that the market for financial services is still confined to a handful of wealthy or technologically sophisticated users. It is unclear how rapidly the habit might spread beyond these groups.

- There are widespread concerns about security. People are reluctant to entrust their financial affairs to an unfamiliar and potentially insecure medium. There is also a lack of confidence in the Internet as a place to do business. Rightly or wrongly, users are afraid of being defrauded. A common question is: “Who is in charge?” The answer is nobody. Conservatism on this score will hamper progress and sustain demand for traditional services.

- Although traditional financial services providers are keenly interested in Internet developments, most of them are still “learning not earning” – watching closely, rather than pitching in with new products and services. The majority of banks still have non-interactive “information only” Web sites. There are virtually no financial services specifically tailored for the Internet, only traditional services in electronic form; to date, financial service providers have been reluctant to pass on the potential savings of the Internet to customers for fear of cannibalizing traditional products.

- While most financial services can theoretically be delivered over the Internet, in practice the range is limited to those which are capable of being automated to a relatively high degree: financial information, account statements, regular payments, and simple loan, savings and investment products.

- There is still no universally convenient means for making payments and transferring money across the Internet. In particular, credit cards, currently the most commonly used means, are uneconomic for small payments and are bedevilled by the perception that they are insecure.

- The technological unreliability of the Internet remains a problem. Many people still find it slow and difficult to navigate.

- Regulation may be the key obstacle. The Internet exposes many of the existing gaps in financial regulation, particularly the territoriality question: how can protection be offered to consumers who use the Internet to bank or invest in another jurisdiction? There are also serious issues regarding disclaimers and health warnings that need to be addressed.

Some of these obstacles could be lowered quite quickly through initiatives by financial services providers or regulators. For example, the development of a truly revolutionary new Net-based financial product would widen the market dramatically, as the spreadsheet did for personal computers. The technical performance of the Internet would also be improved with better browsers and more user-friendly Web sites. At least some of the regulatory obstacles might be overcome through a more co-ordinated approach by regulators. The report makes a number of recommendations in this area.
The Internet and Financial Services

Improvements in the means of payment and settlement across the Internet are also in the offing through the development of electronic cash systems, particularly those not requiring centralised accounting. These systems are probably essential to the development of Internet commerce in general, and are discussed at some length in the report.

One conclusion of the report is that security concerns are more a matter of perception than fact, at least so far as retail consumers are concerned. Encryption and secure transmission services are increasingly available for money transmission. A more pressing concern is the security of computer systems against hackers and criminals: Internet crime is a growing problem – though one on which there is surprisingly little quantitative data.

In the end, “cultural” issues (i.e. people’s attitude towards the Internet) are likely to be the biggest obstacle to change. Until consumers become totally comfortable with the Internet, they won’t use it as a mass medium – but it won’t become a mass medium until far more people use it routinely. The report stresses that traditional financial service providers, particularly banks, could play a major role in promoting consumer confidence in the Internet by lending it their name for integrity and soundness through their involvement as service providers and guarantors. In fact, there may be a major business opportunity for them in providing authentication and verification services.

One of the central conclusions of the report is that the Internet and financial service providers have strong overlapping interests. The Internet needs financial service companies to supply the infrastructure for electronic commerce and to underpin its credibility. For financial service companies, the Internet poses a threat, but also a major new business opportunity.
SECTION ONE: OVERVIEW

People in the financial services industry around the world view the Internet with a mixture of fear and fascination. They sense that it contains the seeds of something revolutionary that could shake their business to its foundations. But is it good news, or bad - a threat or an opportunity? Will the Internet be the final nail in the coffin of traditional High Street banking, or is it the dawn of a new era of virtual finance, cyber-markets and electronic currencies? Might it even be none of these - just hype, the stuff of spotty technophiles and lowbrow futurists?

This report attempts to answer these questions by examining the Internet's impact on the three key areas of the financial services industry: banking, investment and insurance. It also looks at some of the wider issues raised by the Internet: payment systems, security, regulation and the risk of financial crime. Finally, it tries to draw some conclusions about the importance of the Internet for this enormous business sector: will it make a difference, and if so, where and how?

The report is written more for the financial services practitioner than the technologist. It assumes that the reader's basic familiarity is with the financial system rather than the Internet, and that his main interest is the future of the finance industry. Those with a technology bent may therefore find some of the explanatory sections superfluous, but they should bear in mind that the Internet is still a new world to the great majority of people in the finance business.

A word of warning: The way our eight working groups were structured, and the fairly broad terms of reference that they were given, means that they sometimes came to conclusions that were inconsistent - perhaps even incompatible. Since the individual chapters of this report reflect the views of the groups who contributed to them, we have not tried to obfuscate the areas of difference. Although, by the very nature of volunteering, most working group members are positive about the future of the Internet as a medium for the provision of financial services, a few sceptics did creep in - and the degree of enthusiasm was different both within and between groups. In these circumstances, any attempt at synthesis is inevitably fraught with difficulty.

What is the Internet?
The Internet is an informal worldwide network of computers (and of computer networks) which links many millions of users: individuals, companies, academic institutions, governments, etc. It constitutes the world's fastest-growing medium for information exchange, commerce and financial dealings, and especially electronic mail.

The Internet is not a communication network in its own right. It operates through the worldwide long-distance telephone system and on dedicated fibre-
A brief history of the internet: The Internet’s origins lie deep in the Cold War, when California’s RAND Corporation turned its talents to planning for a post-holocaust world. How could US government agencies communicate after a nuclear attack had wiped out any centralized computer systems? The glimmerings of an answer came with a 1962 article by Paul Baran outlining the idea of “pocket-switching” — in which a computer message that was supposed to go from A to B would be broken into packets. Each of these packets would then make its independent way to B — not necessarily by the same, or even the most direct, route. Rather, by a process of trial and error, packages would be tossed from computer “nodes” to “nodes”, eventually ending up at B — where they would all be reassembled. This idea of a decentralized network, where computer systems are hooked up, almost anarchically, to one another — so that, even if half are blasted to atoms, the rest can still move messages around — quickly attracted the attention of the DoD’s Advanced Research Projects Agency. ARPA’s head computer guy, J. R. Licklider, was quick to see the potential, and the agency started trials in 1965 (with assistance from Donald Davies at the UK’s National Physical Laboratory) into the operationalization of packet-switching. By 1969, the DoD had commissioned a research network involving UCLA, SRI, UCSB and the University of Utah that was known as ARPANET. Academics found ARPANET irresistibly sexy — using it for everything from long-distance computing to gestalt. The result was that it grew exponentially, particularly after TCP/IP (the brainchild of Vint Cerf) became the standard for communication between almost all networks. By 1976, the DoD started to get worried that the Net was turning into a giant academic boondoggle, and it reassessed its control through its Defense Communications Agency. That put a damper on the kind of institution that could join — though it didn’t stop development of e-mail as a standard product by 1976. What it did generate was the growth of other (mostly academic) networks, like CSNET, BITNET and USENET, using the same decentralised approach — all of which then hooked up to ARPANET. By 1982, the military gave up and established its own Defense Data Network, which took over the military portions of ARPANET (by then known as MILNET) in 1983.

Nineteen eighty-three was also crucial in that TCP/IP became the single standard for communication between computers in this network, giving connectivity a big boost. The next big boost came with the National Science Foundation’s state-of-the-art NSFNET. This was set up in 1984 and was repeatedly upgraded, thereby setting the standard for all other networks. By 1989, the number of host computers was over 100,000, and at least eleven foreign countries (including the UK) had plugged into NSFNET. Critical mass had been reached.

ARPANET disappeared in mid-1990 — and no one noticed. The Internet was in full flow and private companies (including several set up by ARPANET pioneers) were busy selling Internet connections. The problem was that the Internet’s rapid growth and anarchic structure made it very hard to find a way through — hence increasing effort was put into simplifying it and providing guides. The first really effective tool was Archie, developed at McGill University, which spawned more sophisticated navigators like Gopher and WAIS (and, ultimately, all the commercial search engines used today).

The next big breakthrough came from a Brit, Tim Berners-Lee, working at CERN in Switzerland. His contribution, originally intended to help academic physicists, was the World Wide Web. This is a subset of the Internet, where sites are linked by Universal Resource Locators, which allow the use of hypertext mark-up language to connect computer “sites” (an old idea, much expanded by Berners-Lee). The ease with which the Web can be browsed, and the ability to identify sites easily and accurately (and to standardise those sites), has made it the most user-friendly part of the Net — and the most attractive to business users.
optic lines. Most subscribers gain access to it through a local Internet Service Provider (ISP) -- in the UK, Pipex, Demon, ClaraNet, etc. -- or a full-service network such as Compuserve and America On-Line. Access generally also gives users an address where they can be reached by any other individual on the Net via e-mail.

The Internet is an unregulated system without centralised control. No one owns it, no one manages it and no one (yet) polices it. What holds it together is a series of international standards and protocols which permit different types of computers, anywhere in the world, to "talk" to each other. The most widely-used of these is hyper-text markup language (HTML). This underpins the World Wide Web (WWW), which now provides a standard infrastructure for most of the finance-related activity which takes place on the Internet. The WWW enables users to establish a presence on the Net by setting up a "site". It is now estimated that there are 250,000 commercial sites on the Web. It also allows them to navigate the worldwide system, visit other sites, talk to other users and tap into the thousands of databases which are now available via the Web.

There is no doubt that Web technology is exciting. Sites can now mix print information with graphics, sound and even movies. They can also be interactive. Thanks to HTML, individual sites can be linked -- which means that getting around the Web (or "surfing") can be as easy as clicking a mouse. This creates "threads" of sites -- all connected by the commonality of a single subject or area of interest.

But the Internet is not just the WWW. There are other networks embodied in the Net -- for instance Telnet, which allows a user to gain access to any connected machine anywhere in the world (password permitting). And there are thousands of "chat rooms" and "news groups" that operate outside the Web, and which often serve as a refuge for the most technologically sophisticated "Net surfers" -- those who figure the user-friendliness of the Web attracts a down-market crowd.

Some of these can be very sophisticated indeed. Increasingly, chat rooms (which can cover topics from politics to palaeontology) are incorporating videos and graphics, and are becoming an on-line conference facility. Equally, there is a world of on-line games out there -- sometimes with as many as 10,000 people playing simultaneously, all flat out to win.

The Internet today
It was estimated at the beginning of 1996 that the number of Internet users was 35m worldwide and that this figure was growing at the rate of nearly 50 per cent a year. If this continues, by early next century there will be several hundred million Internet users -- including all the world's governments, most corporations and academic institutions -- as well as an entire Internet-based

---

The Internet and Financial Services

industry which is as yet only in its infancy. In parallel, the number of companies selling goods and services on the Net is expected to double every year.

These spectacular predictions are being fuelled by many factors:

- the growth of public awareness of the Internet;
- the proliferation of increasingly user-friendly technology to access and search the Net;
- the supply via the Internet of useful new services, such as shopping, entertainment and education; and
- the growing use of the Net as a medium for communication.

That said, the Internet also has its sceptics. Some believe, for instance, that its economics are being obfuscated by the willingness of many service suppliers (particularly in the financial services and publishing areas) to view it as a loss leader. At the moment, of the major financial information groups, only Dow Jones charges the full cost of access to its services. When others (e.g. the Financial Times) adopt the same policy, the Internet could lose some of its appeal.

There are also those who believe that the Internet's potential is vastly exaggerated, that much of the "information" available on the Net is of doubtful real value, and that its growth is being fuelled by a self-interested technology industry, rather than by genuine demand. After all, Associated Newspapers closed down its Internet recruitment agency, PeopleNet, in April 1997 after just a year, despite spending more than £3 million on software alone. These doubts feed much of the uncertainty that exists about the Internet: is it hard, or just hype?

The Internet: hard or hype?

Not surprisingly (given that they were self-selected), our working groups had little difficulty answering this question. One of their central conclusions is that the Internet could have a very large impact on the financial services industry – and it is hard to disagree. In areas susceptible to technological innovation, like retail banking, it could even bring about revolutionary change. Moreover, the Internet is already being widely used in the financial field:

- to supply information about financial markets (interest rates, stock prices, company analysis, currency rates, etc.); and
- to deliver basic financial services (e.g. management of personal accounts and investment portfolios).

In these areas, our working groups see scope for a considerable widening and deepening of Internet use, leading to profound changes in the finance industry itself: new structures, products and pricing. They also identified demand for new types of financial services arising from consumers' growing use of the Internet for banking, investment and commerce generally. All this is foreseeable with the technology that is already available – and, to some extent, it is already beginning to happen.
The more difficult question is whether these changes will favour conventional suppliers of financial services (i.e. banks, stockbrokers, insurance companies) or a new generation of Internet-based companies. The sense of many of our working groups was that traditional suppliers have strong inbuilt advantages (i.e. credibility, famous brand names, experience of key Internet issues such as security) which will equip them well to meet new challengers, no matter how aggressive and technologically adept. However, these strengths should not be taken for granted in the Internet world where armies of innovators are busting to assail the smallest problem – and where a technological lead can quickly become a liability as the technology moves on.

Our working groups also identified hurdles which could hold up the growth of financial business on the Internet. Chief among these is the perception of insecurity in such an open communications system. Gaps in regulation, particularly consumer protection, are another reason (perhaps less well understood) for consumer wariness. Third, the technology, despite all the acclaim that is heaped on it, is still surprisingly slow and difficult for the neophyte to use. The Net will never achieve anything like its full potential by appealing only to the committed “Net-head”. Unfortunately, those who are pushing forward the frontiers of the Net still don’t seem to give simplicity and user-friendliness the priority they deserve.

**Relevance of the Internet to financial services**

The Internet has many capabilities and it is important to be clear which of them are relevant to the financial services industry.

The Internet may have started out as a joint venture between academia and the US military, but now it is essentially a marketplace for goods, services and information. It is also, however, a channel of communication and a means to access data. Our working groups concluded that these features not only make the Internet highly relevant to financial services, but in some respects a natural partner. Financial services may even be one of the businesses best suited to the Internet, along with publishing, education and communications.

The main points of relevance to the financial sector are:

- **The Internet's universality**: Before long, everyone who has a telephone and a PC will be on the Internet, or capable of being on it. Initially, those who take advantage of it will tend to be wealthier and better-educated – people who are natural clients of the financial sector.

- **Its suitability for financial service providers**: Unlike merchants who sell physical goods, the finance industry deals in dematerialised services, most of which can be supplied electronically.

- **Its flexibility**: The Internet is suitable for most of the services provided by the financial sector – information, payments, provision of credit, purchase and sale of securities, dealing in financial markets.
The Internet and Financial Services

- **The convenience:** The Internet can be accessed from anywhere, at any time of the day.

- **It exists:** The Internet is already here, relieving the industry of any need to build its own networks. Indeed, many financial companies already use parts of the Internet as “intranets” for their private communications.

- **A glaring business opportunity:** First, the Internet needs security – and security is one of the things a bank is used to selling. Second, in order to reach its potential, the Net needs better payment systems – and that is something banks know a lot about. Third, the Net is still new: it needs good, solid names to give it respectability and to build up business.

The last point is particularly worth noting: the Internet needs the participation of the financial services industry to strengthen its own standing and capabilities. In other words, the Internet is not a newfangled facility which the financial services industry can choose to ignore. Nor can those who are promoting the Internet choose to ignore the financial services sector. A strong mutuality of interest draws them together.

However, there is another side that needs to be emphasised:

- Many people still have a strong preference for personal contact when conducting their financial affairs. So there may be a limit to the range of financial services that can successfully be offered on the Internet at this time. The more traditional forms of contact – bank branches, telephone etc., even ordinary letter writing – will remain in demand.

- The technical difficulty of finding one’s way around the Web and of locating suitable services should not be underestimated. A lot of effort is going into solving this problem but many feel that user-friendliness still does not get the priority it deserves.

- It is currently very difficult to ensure that people who buy financial services over the Internet receive the same level of legal and regulatory protection as they do in conventional markets. The Internet’s ability to transcend geographical boundaries makes a nonsense of virtually all territorially-based regulation and exposes it to potential abuse.

- The security of transactions conducted over an open network remains a concern. This is more a perceived than an actual problem because the necessary encryption technology is now available. But if people believe that communication on the Internet is unsafe, they will shun it, particularly for money matters.

- Linked to this is the fact that the Internet is, of its nature, an open system – and many users would be more comfortable with a closed system that they can manage. It is possible to “fence off” certain parts of the Internet and to run them as proprietary “intranets” – and that may become increasingly popular. In the meantime, many of the world’s largest insurance
brokers have deliberately eschewed the Net and have created their own proprietary World Insurance Network (WIN) so that they can set their own standards and determine criteria for access. Maybe WIN will eventually be accessible from the Net, but that is not the case at present.

These problems are not insubstantial. In particular, it will take a major cultural change to overcome a personal preference for face-to-face contact, and it may take a major international initiative to overcome the regulatory obstacles. Both will take time.

The technological impact
Despite these difficulties, there is agreement that the Internet has the potential to bring about revolutionary change. But, what does revolutionary change really mean?

The retail banking group's report draws a useful distinction between the impact of hole-in-the-wall cash machines and swipe cards, both of which were seen at the time of their birth as major technological breakthroughs. With hindsight, though, the cash machines did not fundamentally alter the structure of the business, or the bank-customer relationship, except perhaps by reducing the amount of personal contact. Swipe cards, on the other hand, cracked open many of the banks' prized monopolies. In particular, they enabled non-banks to get into businesses such as payments and credit, and through those to invade a large slice of banking territory.

A similar impact is foreseen by many for the Internet:

- **First, the Internet is a new medium that ought to be particularly well-suited to a service and information-based business like finance:** Virtually every financial service is capable of being delivered or transacted over the Internet, at least in theory. The only obvious exception is cash handling, but even that need not be a problem if, as seems possible, the Internet hastens the shift to electronic money. The potential therefore should exist for a large scale transfer of financial services from their materialised form (branches, paper, cash) to an electronic form (Web sites, e-mail, digital money) – if the obstacles to change which have already been mentioned (public acceptance, user friendliness, weaknesses of regulation and security) can be overcome.

- **Second, should the industry undergo this transformation, the economics of the financial services sector would change:** They would shift against traditional suppliers with their "legacy systems" and high regulatory costs, in favour of new suppliers with low costs, technological know-how and a clear understanding of the business opportunities created by the Internet. In this world, traditional suppliers may retain certain advantages from the strength of their brands and their knowledge of the business (e.g. making credit, taking insurance risk, managing security). But would these advantages be enough to safeguard their market position?
The Internet and Financial Services

- **Third, the transformation into an electronic world would create new business patterns and alliances**: The flexible architecture of the Internet allows services to be designed and sold in ways which reflect patterns of demand, instead of being shaped by the traditional supply structures of the past. In other words, institutions like banks, stockbrokers and fund managers may no longer be required in their old form. They could respond by regrouping among themselves or with other service providers to create hybrid products and structures (e.g. bank-broking accounts, retailers and credit suppliers, bancassurance). Since this tendency is already visible in the old world, the Internet will probably accelerate it. Where the Internet will add an extra dimension is by making it easier for non-financial firms to get into the finance business (e.g. information providers and companies in the telecommunications and technology fields).

- **Fourth, the Internet could create much greater transparency in an industry which is notorious for its ability to obscure price comparisons and to get away with wide profit margins**: Using search engines and intelligent agents, consumers (retail or professional) will be able to scour the market for the best savings and lending rates, life insurance terms, etc. This could be devastating for companies who supply relatively straightforward, commodity-type products such as checking accounts, mortgages, PEPs or house insurance. This pressure alone could produce a radical restructing among financial institutions. It could also accelerate the move towards product standardisation, though banks and insurance companies could also exploit the Internet’s technological capabilities to “customise” products and dress them up with added-value features so as to charge more for them: e.g. a mortgage/home insurance/life insurance package with optional rate capping “just for you”.

If the Internet fulfils its promise, it will bring about revolutionary change in two ways: by opening up a new medium for the conduct of financial services and by hastening the transformation of the industry. But while such forecasts are plausible, they have to take account of the obstacles.

**What will drive the Internet?**

Although a large, vigorous and vocal technology and software industry is driving the Internet forward, the little evidence available suggests that the market for financial services on the Net remains small. Even though a recent study by Nielsen Media found that nearly one quarter of the North American population over 16 accessed the Internet at least once during December 1996, as yet few people do their banking and investing through the Net and virtually nobody buys insurance. This will only change if people decide that the Internet really does offer them a better way of managing their financial affairs. What are the prospects for this?

Many of our working groups were confident that the prospects are good simply because of the momentum of technological progress: even if it isn’t yet, the Internet will be a cheaper and more convenient way to do one’s
banking. But the financial services market will be a tough nut for the Internet to crack because of the special requirement for soundness and integrity. This made our groups cautious about how fast such a market might evolve.

However, a distinction should be drawn between the retail and wholesale parts of the finance industry because the Internet is likely to have a greater impact on the first, at least initially. The retail business is primarily a mass market, amenable to product standardisation and automation—all characteristics which suit the Internet. Not only is the Net able to distribute commodity-style products more cheaply than other channels, it is also (paradoxically) able to “personalise” them in small ways that may well appeal to an Internet customer base. Moreover, this applies as much to insurance and investment as it does to banking (viz. the proliferation of ATMs, direct sale motor insurance and unit trusts).

In contrast, the wholesale end of the business (defined here as the capital and equity markets, financial services for large corporations, and the transfer of large payments) is a “bespoke” business, in which a low-cost mass market distribution network is far less important. Moreover, where networks are appropriate, they are already being developed. If the Internet is to have an impact on the wholesale side, it will, at least initially, be more in the area of communication (e.g. the use of the Internet for internal communications, or “intranets”), streamlining the back office, reducing trade confirmation and settlement costs etc. A considerable amount of work is already going on in these areas.

So the driver for the Net will probably be the retail side. Here, one way of assessing the impact of the Internet is to look at the financial services that might be delivered over it. Even though most financial products could in theory be sold electronically, this will almost certainly turn out not to be the case for reasons already mentioned (e.g. concerns about security, need for personal advice etc.). The Internet will be selective.

Which products are most amenable to the Internet? The personal finance working group compiled a spectrum of products in the personal banking and investment areas to illustrate this point. At one end lie those products which are most compatible with Internet marketing—in other words, with automation and electronic delivery. Chief among them is information, which includes quotations (of prices, interest rates etc.) as well as higher value-added forms (analysis, investment research, educational material and even standardised advice).

Slightly less amenable are commodity products like checking and savings accounts, investment portfolios etc. These require a more personalised presentation, but are still standardised and can be automated.

In the middle lie hybrid products which can be delivered in a standard form but require a certain amount of genuine personal attention on the part of the
The Internet and Financial Services

supplier: execution-only share dealing, mortgages, life insurance, long term savings plans etc.

At the far end – and, therefore, least amenable to Net distribution – lie services which require the most individual attention: pensions, portfolio management etc. Although these might be delivered over the Internet (and purchasers may use the Internet to monitor their performance), they need a high degree of personal involvement on the part of the supplier. Indeed, many clients might flatly refuse to buy these services over the Internet.

In the view of the working group, the key point about the range is that the more amenable products are to Internet delivery, the more “commoditised” they are likely to be, and the less profitable they will be. For example, the supply of price information carries lower profit margins than the management of an individual’s investment portfolio.

This points to an important strategy choice for institutions approaching the Internet: the more they do business over the Internet, the more they are likely (at least initially) to find themselves at the low margin end of the market. The Internet can compensate, of course. In the first place, it may be cheap. In the second place, it may boost volume. And, in the third place, it may open up possibilities for cross-selling of other financial products. It may also be possible to add value to even basic commodity products by customising them to some extent. But, notwithstanding all this, it is easy to see a situation in which growth of the Internet could increase polarization in the financial services sector:

• commodity-type products could gravitate to Internet-type delivery systems; while

• more complex personal finance products could continue to be sold on a face-to-face basis.

This is not inevitable. Indeed, some working group members felt that one of the biggest advantages of distribution via the Net is that it could enable the supplier to personalise even commodity products at low cost. (The fear is that, without personalization of services, Internet users will develop no customer loyalty.) But, on balance, polarization is quite likely in the initial stage of Internet provision of financial services.

Will the Internet be cheaper? The research cited by some of our working groups suggests that, on the limited data available, the cost of doing business via the Internet is significantly lower than through conventional channels – as one would expect. Some support for this is provided by telephone banking where, according to the Banking Administration Institute in the US, the annual cost of managing an account is US$43 compared to US$118 in a conventional branch.

The reason for this is that the Internet makes possible a number of important savings:
it cuts down on the need for bricks and mortar;

- operations can be centralised;

- the marginal cost of additional transactions is very small; and

- some operations that were traditionally done in-house by the service provider can now be “outbanked” on to the client’s computer, thanks to new technology like Sun Microsystems’ Java “applets” (mini-programmes that can be downloaded from the Internet on to a PC to perform specific functions).

**Will the Internet gain acceptance for selling financial services?**

There are two broad issues here:

- Will Net technology reach a suitable level of user friendliness?

- Will the consumer ever become sufficiently confident about the Internet?

**User friendliness:** All our working groups agreed that the Internet still has some way to go in this regard. Net access through the main ISPs is still slow and unreliable, particularly when peak user times in Europe and the US overlap. Many Web sites are harder than they should be to locate and, once reached, many of the more sophisticated ones take a long time to load. In addition, until now, search engines have not been sufficiently discriminating when asked to track down particular items of information. Most of the difficulties are compounded by the fact that (by definition) the average user has equipment with only average capability, which seldom matches the promise of the glossy magazines. But the problem is not only one of technology. Many home pages are poorly designed or over-elaborate, which makes them hard to transmit. (See the personal finance working group’s report for one participant’s experiences trying to track down information about financial products.)

However, the working groups generally expect user friendliness to improve – partly because marketing staff at the service providers are aware of the deficiencies and partly because the “winner takes all” nature of Internet technology puts intense pressure on innovators to come up with the winning solution. The evolution of the Internet is marked by periods of experimentation when little seems to happen, followed by technological “jump starts” as new techniques become standard.

A particular need identified by our personal finance group was for a specialised financial services search engine to simplify the task of locating the right information. Although several useful “link pages” exist – a few even having a site-specific search capability – much more is required in this area.

A further need is for a simple, secure and low-cost payment system capable of handling transfers of relatively small sums of money, preferably in several currencies, so that Internet users can pay for their Internet shopping. Again, progress is being made, albeit slowly. The problem is that too many approaches are currently being pursued – which means that no standard has yet emerged.
The Internet and Financial Services

Confidence: While our working groups believe that user friendliness could be improved quite quickly, they are less certain about user confidence. Research has shown a lack of confidence in the Internet and a lack of understanding of how it works. A common question is “Who is in charge?” The answer is nobody, which is true but disconcerting.

This lack of confidence cannot be remedied by improved software or by more powerful computers. It requires users to become comfortable with the soundness of the system and the people they deal with at the other end - an issue of special relevance to financial services. They also need to be assured that the traditional regulatory and legal remedies exist if they are deceived or defrauded.

From the standpoint of Internet infrastructure, big improvements in system security have already been made. An increasing number of encryption and secure transmission services are available, but they may well cost money and are insufficiently widely known. Moreover, they require a serious commitment by senior management and that may be a problem. Financial regulators are also taking a close interest in developments on the Internet, particularly in measures that could boost confidence such as providing some sort of assurance or “kitemark” for regulated institutions.

Among the ways Internet confidence could be improved are:

- wider publicity for Net security services;
- the encouragement of standard-setting by the industry groups most involved (including financial services); and
- a more active presence on the Internet for household names, so as to give it “respectability”.

In this last regard, the big banks could play a key role in legitimising the Internet as a safe place to do business. Most of them are already on the Net, but users would like to see a commitment to an active Internet presence beyond simple advertising.

Our working groups also recommended that more should be done to educate the public and to dispel fear and ignorance, particularly among older people. From the individual’s point of view, confidence clearly grows with use, but this skews the market towards the more technologically-inclined young – which may not be the most lucrative segment for financial service suppliers (at least for the next few years). From the corporate point of view, the conviction of the Internet’s value as a commercial tool also grows with use. But strategy-makers tend to be senior people with little Internet experience. The people in companies who really do understand the Internet are those in the information technology departments who are frequently not represented at board level and who are, in any case, less able to articulate its commercial potential. The corporate boardroom needs more Internet users.
Overview

Because of these constraints, a number of our working groups did not really expect to see the full potential of the Internet realized in the short term. In particular, they did not anticipate growth of the mass Internet market for financial services in the next few years – though no one ruled out dramatic change later on. In this respect the financial services industry differs from other areas of Internet use such as entertainment, where business growth is expected to be immediate and explosive. Indeed, the Internet-based market for financial services may be confined for some time to two relatively small, albeit potentially very profitable, segments: the wealthy and the technologically sophisticated.

Present strategies
What are institutions doing at the moment, particularly in the UK? Virtually all the major financial institutions have displayed a strong interest in the Internet, but almost all are wary of making a heavy commitment at this stage. In the UK, most banks, insurance brokers and fund managers have opted quite sensibly for a “toe in the water” approach, so that they can observe developments and think about their longer-term strategies. The majority still have “information only” Web sites, which are advertisements rather than platforms for real transactions. Our personal finance group ran a straw poll of financial service providers and discovered that their Internet sites were attracting little new business; but the providers claimed that the experience was nonetheless useful.

No institution has yet, to the knowledge of our working groups, developed special products for the Internet (i.e. which are more than traditional products in a digitised form) – though it is true that the Net can already bring to the level of the individual investor near-real time quotes and portfolio management tools that, until now, have been the preserve of institutional investors. And, certainly, the US experience suggests that the Internet has given a great boost to personal finance products like Quicken and Microsoft Money.

Who is really going to take the leap and risk real money on a Net presence?
In the US, there are a few Internet-based financial service providers (e.g. First Virtual and Security First) and plenty of banks and brokerages (e.g. Wells Fargo and Fidelity) that are expanding, and publicizing, their commitment to the Net. But no one is putting megabucks into it anywhere – yet. Same in the UK. There was a great deal of hype about BarclaySquare and Buckingham Gate, but they were low-risk shopping malls that were intended primarily as a learning experience for the sponsoring banks, Barclays and NatWest. The Royal Bank of Scotland’s Internet-based personal banking system is the first major commitment in the UK, but it is still too early to assess how high a priority it is being given within the bank (let alone what customers will make of it).

Despite all this cold(ish) water, many European financial institutions are expected to increase their commitment to the Internet over the coming years by making their sites more interactive and capable of handling transactions. A
The Internet and Financial Services

survey of 37 top European banks by consultants Booz, Allen & Hamilton in 1996 found that 78 per cent of them planned to have special services available over the Internet in the next three years.¹ These could include the ability to apply for a bank account and to provide information about balances, account transfers and bill payments – all on-line. More than 70 per cent of the banks planned to provide some of these services within a year.

So we may be at the point of a big commercial breakthrough.

 Threats and opportunities

The greatest threat to existing financial institutions is that the Internet will edge them out of the market. This could happen for several reasons:

• because they are slow to adapt;

• because the electronic medium makes them obsolete; or

• because they cannot compete in the new environment.

However, our working groups were far from negative about the prospects. All of them commented on the fast-growing awareness of the Internet within the financial services industry, particularly banks. They also identified significant business opportunities for financial institutions on the Internet: some new and some coming from the translation of traditional services into electronic form.

Intermediaries: Our working groups thought that stockbrokers, insurance brokers and financial advisers were among the most exposed because they live by creating expert links between suppliers and buyers of financial services. The Internet could weaken the need for these links by giving the consumer the means to find things out for himself and then to act upon his own decisions. If he can read stock prices and execute his chosen transaction through an on-line discount broker, why pay the expense of a full-service broker? If he can call up all the motor insurance quotes in the market and buy the one he likes best, why should he go through an insurance broker? If he can obtain information about unit trusts – their price, their performance and how to buy them – he does not need a financial adviser.

Some of these groups are especially vulnerable because they have been slow to embrace new technology: independent financial advisers are said to be particularly resistant to change, not least because few have substantial financial resources.

But there are contrary views to the one just described. If the Internet opens up access to vast amounts of information, it can be argued that the need for someone who can make sense of it grows rather than diminishes. The stockbroker and the insurance broker could discover a new existence as suppliers of value-added information services; the IFA could become his clients’ personal guide to what is on offer on the Net – an “info-mediary”.

Personal finance providers: There seemed to be agreement among our working groups that this is where a great deal of activity will gravitate. The Internet will give the individual more control over his financial affairs: he will be able to obtain information and execute transactions over the Internet; at the same time sophisticated personal finance software packages will enable him to centralise his financial affairs on his PC. Demand for personal finance services is already growing, but the increasing emphasis on private welfare provision means that more and more individuals will be drawn into the market over time.

Structurally, the growing role of personal finance software products could mean that these become the focus of an individual’s financial affairs, rather than the institutions he deals with. He will “log on” using Quicken, rather than other software or on-line interfaces that his broker or his bank may supply. And the result may be that his “loyalty” is to Quicken, and not to the bank. Microsoft’s attempt to buy Intuit, the company which owns Quicken, suggests that others hold the same view that the key to the customer lies in the proprietary interface rather than through the particular product that the interface permits the user to access. However, what was also clear from our working groups is that the Internet needs to become a lot more user-friendly if it is to make major inroads in this area. There are new developments in browser technology that will help, but at present the Net is by no means a surfer’s paradise.

Banks: The banks stand to lose a lot to the Internet, but new business possibilities are also considerable. Moreover, our retail banking group felt that the evolution of the Internet is still at a stage where banks can take the initiative to protect and strengthen their position, though the moment of opportunity may not last long.

As some see it, the greatest threat is that the Internet could remove the need for banks altogether by taking the intermediary out of the credit process. It is theoretically possible for the Internet to put lenders (i.e. people with money) in direct contact with borrowers, so that they can avoid paying banks for standing in the middle. This has not happened yet; nor is it on the immediate horizon. But it is worth mentioning because it also highlights one of the banks’ strengths: just as the insurance broker’s ability to interpret information may be a strength rather than a weakness in an information-rich environment, the banks’ understanding of credit and their ability to take on intermediation risk could turn out to be an asset in a world where sources of credit proliferate.

Two areas of potential new business for banks stand out:

- **Payment and settlements:** One of the central conclusions reached by our working groups was that sophisticated payment and settlement systems are essential if the Internet is to establish itself as a serious medium for electronic commerce, and that this represents a key opportunity for banks. Unless people and businesses can pay quickly and simply for items they buy over the Internet, its appeal will remain limited.
The Internet and Financial Services

At the moment, most retail commerce over the Internet is paid for by credit cards, just as in the real world: buyers key in their card numbers and the item is charged to their card account. But this has several disadvantages:

- First, it is perceived to be insecure. Even if a secure server is used, the number appears to be sent down an open telephone line, where it is widely believed that it can be intercepted. Clearly, this is no more insecure than conventional shopping, which requires the merchant to send his customer’s card number down a phone line for authentication. But this point does not appear to cut much ice in the new and slightly frightening world of Internet shopping. Nor does the growing availability of encryption yet appear to have made much impact on consumers.

- Second, and potentially more important, it is expensive. Most plastic card systems are centrally accounted, which means that all transactions have to be processed by the card issuer and then settled by the purchaser through his monthly statement. It is estimated that the smallest transaction that is economic in a centrally-accounted system is around US$5. But this is many times more than the few cents (or even fractions of a cent) that content providers plan to charge users to look at information pages on the Net.

The need therefore arises for much cheaper payment systems. The answer may lie in stored-value cards (like Mondex) or other forms of electronic cash that do not need to be centrally processed. Like ordinary cash, stored-value cards can transfer value from one person to another without reference to a central issuing or accounting authority. The same is true of other forms of e-cash (e.g. DigiCash): e-cash is essentially nothing more than a series of electronic blips which can exist on plastic cards (telephone tokens are an example) or the disc drives of computers, and which can be readily transferred from one electronic purse to another. In a typical transaction, a person might extract cash from his bank account by dipping a plastic card into an electronic terminal. He would feed that cash into his computer, where it would become available for purchases on the Internet. He would then instruct his computer to transfer the required sum to the merchant over the Internet link. Electronic gadgets at either end would ensure that the money really had passed and that it was genuine. In the not-too-distant future, various stages of this process could be eliminated: the user’s computer could be directly linked to his bank account and would be able to transfer e-cash from it straight into the merchant’s account.

The point about all forms of e-cash is that the marginal cost of transferring value from buyer to seller is virtually zero once the two sides have invested in the necessary equipment. This opens up considerable possibilities for Internet commerce because it allows tiny transactions to be paid for, e.g. ones worth only pennies or cents.
The real question is whether these e-cash systems will be supplied and serviced by banks or by non-bank newcomers. The banks clearly have an interest in maintaining a strong position in this area: it is a natural business for them, and if they lost it a key part of their franchise would be gone. However our working group on payments and settlements noted that there is no strong reason other than consumer confidence why payments services should be supplied by banks. Big inroads are already being made by non-banking companies (like Visa and Mastercard) in micro-payments, secure transmission systems etc., suggesting that this will be an area of widespread and growing competition.

A related issue is the ability of payment systems to deal in several currencies. Since much trading on the Internet should naturally occur cross-border, any truly useful payment system must be able to convert the purchaser’s e-cash into whatever denomination is demanded by the seller. Mondex goes a long way to meeting this requirement: currently, it can handle five currencies (although in its trials it was restricted to sterling).

- Authentication: Another precondition for successful Internet commerce is that dealers and dealings should be sound. Many potential users fear this may not be the case, particularly when doing business with unknown entities in far-off lands. While secure e-cash systems may help overcome some of these concerns, our working groups saw a strong need for credible organisations to lend their names to transactions and to provide an underpinning of confidence. They also saw this as a natural role for banks.

The requirement is, essentially, for someone to reduce the risk of dealing on the Internet by taking it on himself for a fee, which is why some people have termed this role “risk management”. The manager’s role might include verifying the parties to a transaction, guaranteeing payments, authenticating sales claims etc. – Is the merchant really who he says he is? How do you know he will deliver? How can he be sure he will get paid?

That a need for such services exists may be seen from the fact that some large organisations are already supplying it. For instance, AT&T has offered to refund anyone who is defrauded while using its Universal credit card over its Worldnet system. The US Postal Service is also examining various verification procedures, including electronic post marks. In addition, a number of countries already have, or are exploring, the legislative infrastructure to permit so-called digital signatures. These will require licensed bodies, known variously as trusted third parties (TTPs) or certification authorities (CAs), to certify signatures and to maintain a registry of issued certificates.

Banks have a number of qualifications for this role. They are credible and generally sound institutions. They already perform similar functions: trusteeship, safekeeping, refereeing etc. And they have the systems to store and process information. The direct commercial value of this business (to
The Internet and Financial Services

the insurance industry, as well as to banks) would probably lie in the fact that the perceived risk of dealing over the Internet is greater than the actual risk. The authentication service could therefore be priced to exploit the gap between the two. However, our working groups saw strategic benefits as well: a presence in this business might help protect the banks’ payments franchise at a time when it could come under serious threat. The revenue would compensate them for the loss of float which would result from the shift from multi-day paper-based settlement to instantaneous electronic payment. And the transaction authentication process would also give them a huge amount of information about individuals’ financial habits which, privacy laws permitting, could be used for wider marketing and business purposes.

However, there could be a level of moral hazard attached to this. By providing high profile guarantees, the banks would be in the firing line if anything ever went seriously wrong. They might also foster a public perception that they were “in charge of the Internet” and therefore responsible for everything that happened on it.

Our retail banking working group saw a related role for banks as providers of Internet platforms for their smaller commercial clients such as shops or service companies lacking well-known brand names. These would be more localised forms of the electronic shopping mall concept that is already being operated by a number of banks on a national basis. The clients would derive the advantage of having their names linked to a well-known bank, while the bank would secure the business of servicing their Internet transactions.

Equity markets: It was agreed that the Internet could affect the securities markets in a number of ways. We have already seen the possibility that full-service stockbrokers might be edged out of business by an “empowered” investor. Their place would be taken by execution-only brokers competing only on price. But change could also affect the very heart of the market: the stock exchanges themselves.

The Internet’s ability to bring buyers and sellers together has already raised questions about the need for a centralised marketplace for securities in the traditional sense. Investors, it is argued, could post their bids and offers on bulletin boards or through order matching services, or even do their deals by e-mail. This could occur in both the primary and secondary markets. Companies might even issue shares directly to investors rather than go to the trouble and expense of hiring investment banks and underwriters. In a much-quoted example, a small New York brewery, Spring Street Brewing, did just that in February 1996 in a US$1.6m deal which was approved by the SEC. Even though it seems unlikely that this practice will catch on quickly among blue chip stocks, if only because the risks of failure are huge, the Spring Street deal did provide a possible glimpse of the future.

The issue for securities markets is whether trading could become more efficient on the Internet. The cost of execution would certainly be lower, because
trading and settlement could be totally automated. The Internet's global reach could also create a much wider and more liquid market for stocks, open all hours, everywhere. But might this result in more fragmented, and therefore less efficient, markets? How would an investor who dealt through a bulletin board know that he was getting the best price? How would the rest of the market learn about the amount of business that was being done in a particular stock, and at what price? How would such markets be regulated?

The logic for some sort of centralised market may, therefore, remain compelling — and, indeed, such a market could exist on the Internet, with prices available to all. If so, it might be a more democratic market in the sense that the small investor had access to precisely the same information, and at the same time, as the biggest market maker, and there would be less opportunity for the heavy hitters to manipulate prices.

Creating the conditions for Internet commerce

Internet commerce will not take off on its own accord: it will need the right framework. There are several areas where our working groups saw a need for further work by government, the technology industry and service providers. In particular:

- **Clearer regulation:** The scale and speed of the Internet's growth has raised a number of important regulatory concerns, many linked to how consumers can be protected in its fast-growing and essentially frontierless world. But while the novel character of the Internet makes these problems look large and threatening, many of them are really familiar issues in a new guise.

Our working group on regulation took the view that while the Internet had its particular problems, they were not insurmountable and certainly did not mean that the Internet is an anarchic world to be avoided by law-abiding citizens. What is new about the Internet is the enormous growth it could fuel in crossborder transactions and in the use of electronic payment systems — both areas where there were already tricky regulatory questions. Together, these call for a more proactive approach on the part of regulators, and possibly even an international framework to replace the hodgepodge of national regulations. Given the limitations of organisations like IOSCO, this may seem like a pious hope but it may be the best bet if the Net is to realize its potential.

Financial regulators have been grappling for some time with the difficulties created when a financial service provider (a bank or fund manager) promotes its services in another country: the territoriality issue. In many cases, someone buying those services might not enjoy the regulatory protection of either his own authorities or those of the provider's country. In the UK, various regulations and practices have been developed to cope with this problem: it is illegal, for example, for a foreign bank from outside the EEA to tout for deposits unless licensed in the UK, or for anyone to issue an investment advertisement which has not been approved by an
authorised person. But does advertising in international newspapers, which happen to circulate in the UK, amount to "soliciting for business" in the UK? By the same token, does a New York-based stockbroker’s Web site amount to conducting business in the UK if it can be accessed from London? More complicated still, what if that New York stockbroker’s Web site actually exists on a server based in the Bahamas? Our working group recommends that the law should be clarified to state that such sites would only be subject to UK law if they were specifically directing their services at the UK market. One solution to these problems might be for regulators to reverse the present presumption that a foreign institution whose Web site is accessible from the UK is effectively moving into UK regulatory jurisdiction. If they made the opposite presumption that someone who responds to a solicitation from abroad is, effectively, leaving the UK—the problem would be greatly simplified. The solicitation issue would be removed and the investor would be deemed to have passed into the service provider’s regulatory jurisdiction.¹

The geographical flexibility of the Internet also opens up greater opportunities for regulatory and legal arbitrage: locating services in lightly regulated centres to escape compliance costs. It remains to be seen, though, whether this is a profitable pursuit. It is generally the case that centres with a poor reputation tend to attract less business than those which are well-regulated. Within the EU, the Internet provides a classic case for "single market" regulation which the Commission is now pursuing.

Another major area of regulatory concern is electronic documents. Paper documents are relatively straightforward: they can be identified and handled, and, once printed, are hard to alter. Electronic documents exist in cyberspace; they can be easily manipulated and altered. Furthermore, most legal documents are intended to be read as a whole. Electronic search engines, hypertext links, "bookmarks", etc. provide a way of skipping through documents, thereby potentially bypassing key passages such as "health warnings". Should this be disallowed to ensure that investors reading an electronic prospectus are forced to see these warnings? Should health warnings be printed on every page? Should publishers of electronic documents be required to keep records of every version that existed, and the exact time of any changes? Again, there is a danger that over-strict interpretation of regulations that were originally intended for print media will result in immensely burdensome controls, and an impossible task for regulators.

Remedies can, and doubtless will, be proposed to deal with these problems. But they raise a broader issue of how tough Internet regulation should be. Does the novel character and wide sweep of the Internet require it to be more heavily regulated than conventional markets? This would imply that

¹. A Financial Times story on May 1, 1997 suggests that the Securities & Futures Authority still takes the view that all sites that can be downloaded in the UK should comply with UK rules.
the risks are greater, and need to be more tightly controlled. Or is it right, as a matter of principle, that the Internet should be no more severely regulated than other markets with which it competes? This would align with the view that the regulatory issues raised by the Internet are, fundamentally, little different from those with which we are already familiar. A third possibility is that the Internet could be viewed as an opportunity to reduce regulation. This is a harder proposition to accept. But if the strength of the Internet is its universality, there might be public benefit in ensuring the widest and freest access to it.

This view was echoed by Sir Andrew Large, the chairman of the Securities and Investments Board, the UK’s regulator of the securities markets. Towards the end of 1996, he said: “New technology always poses a challenge. But its benefits are manifest, and our task is the exciting, albeit often difficult one, of finding solutions that not only provide investor protection but, importantly, work to support progress rather than impede it.”

To date, regulators have been reluctant (in some people’s view, slow) to take action to deal with the Internet. Three of our working groups recommend a more proactive approach. Our regulatory group says that regulators should take the opportunity presented by the Internet to address a number of outstanding problems: the status of foreign sites, the special requirements of electronic documents, and the need for closer cooperation between different types of regulators (banking, insurance and investment) because of the fluidity between these areas that the Internet creates. Our personal finance group felt that firms authorised by UK regulators should have an official “kitemark” to establish their credentials on the Internet and to differentiate them from the “cowboys” — an idea that regulators are examining though it would need to avoid the problem of moral hazard. Our insurance group commented that the Department of Trade and Industry, which regulates insurance in the UK, seemed to be more concerned with the solvency of insurance companies than with the medium through which they marketed their services. The group felt this was a potentially dangerous view because of the major impact that the Internet could have on the market.

- **A better legal framework**: As with regulation, most of the legal precedents relating to the Internet are derived from print media, and some shortcomings are obvious. For instance, in the US, material on the Net that may be legal in one state can be illegal in another (because of local community standards) — making the provider of a Web site liable under, say, Louisiana law every time someone in Louisiana accessed a page that would be quite acceptable in California. In addition, there are several legal issues that relate specifically to cyberspace, e.g.:

1. From a speech given to The House magazine Conference, “Big Bang: Ten Years on”, October 29, 1996.
The Internet and Financial Services

- the status of digital signatures (which is only just starting to be addressed, even in the US); and
- the broader status of electronic contracts.

There is also an underlying problem under English law in that the "theft" of information is not a criminal offence. This has made it extremely difficult to get convictions in English courts for offences like "hacking". On top of this, many offences on the Internet are initiated from countries where the law is still rudimentary, and extradition is impossible.

Certainly, crime on the Internet is a serious issue – though it is significant that no one knows how much there is of it (the CSFI has made its own proposal for a computer crime clearing house to provide an answer to this). There is already a growing industry devoted to preventing or detecting Internet crime – which, paradoxically, means that objective analysis is getting harder to come by. But a big step forward would be closer international co-operation, and, nationally, among the various law enforcement offices in the UK.

- **Better security**: Security is a key issue for the further evolution of the Internet. The widespread (if inaccurate) perception that the Internet is inherently insecure is holding back users and preventing the growth of commerce, particularly on the financial services side. However our security working group drew an important distinction between two aspects of the security issue:
  - the public’s perception that payment systems on the Internet are insecure is almost certainly false; but
  - the fact that the Internet operates on open communication lines does mark a step level change in the threat to computer systems.

Taking the first of these, the group argued that financial service providers are used to dealing with security problems, and that there are no major obstacles to ensuring that it is safe to conduct financial transactions over the Internet. A considerable degree of security is already built into most financial packages in the form of standard encryption algorithms. When one considers how insecure non-Internet payment systems are, even the rather basic security built into, say, Quicken or Netscape ought to increase consumer confidence, not diminish it. Moreover, under pressure from suppliers and the financial services industry, the US is progressively relaxing its restriction on the export of stronger encryption. Coupled with initiatives like the UK DTI’s key escrow system (which would provide very strong asymmetric encryption, with the DTI holding a copy of the key), security of payments really should not be a problem.

However, system security is a trickier area. Even before the growth of the Internet, hacking and computer viruses had become a serious problem.
The advent of the Net means a huge increase in connectivity – and that greatly increases the risk that systems are exposed to. Unfortunately, as the Net has developed, so has the availability of sophisticated hacking tools – meaning that any dedicated hacker can have access to some of the most sophisticated programs in the world. Coupled with an often cavalier attitude to in-house security procedures (modems installed without letting anyone know, etc.), this means that few computer systems can be considered absolutely safe. Even where such systems are well-managed, viruses or “Trojan horses” can all too easily be imported via floppy discs or downloaded from the Net itself – or, horrors, they can be deliberately installed by malicious or corrupt operators, perhaps even external contractors brought in to maintain a system.

A lot can be done to reduce the threat to one’s computer system, but there is no doubt that “connectivity” significantly increases any system’s vulnerability.

- **Better technology**: One of the recurring themes of most of the working groups is the need to make the Internet more user-friendly. One way to ensure this is to harness technology more effectively. Our personal finance group was deeply unimpressed with the way that one major search engine tried to navigate the Web in search of basic financial products. Improvements are certainly in order here, and they may be forthcoming. So-called “intelligent agents” (often based on neural network technology) are increasingly available as software packages and can be “trained” to search out material specific to the interests of a particular user.

There are also several Web sites that specialize in financial services, offering hundreds (even thousands) of links to financial sites. These services are now growing rapidly.

It is true, of course, that software to simplify use of the Net can come to pose a threat to established suppliers. As noted earlier, subscribers may develop a loyalty to the program rather than to the service providers. This is probably an insuperable problem, but the finance industry might usefully work co-operatively on some sort of special purpose financial search engine to prevent the software suppliers from interposing themselves between them and their customers.

**Social issues**

By and large, our working groups have eschewed broader political and social issues relating to the Internet. Given that this is supposed to be a practical guide, that is surely appropriate. However, there is no doubt that public policy issues are involved. For instance:

- **Confidentiality**: The debate over encryption has to balance the need for security against the public interest in tracking crime, stopping money laundering, etc. Who will control the encrypters? And, if, in the UK, it is the DTI (through its key escrow proposal) who will ensure that the
The Internet and Financial Services

Department itself does not just go on fishing expeditions through confidential material?

- **Taxation**: Internet commerce of any sort *can* facilitate tax avoidance. It will become very easy to purchase de-materialised goods and services on a cross-border basis, thereby avoiding custom duties, VAT, etc. How will governments around the world respond to this?

- **Monetary policy**: Further out, any e-cash scheme will have consequences for the management of monetary policy. So far, the Bank of England (like the Fed) has taken the view that this is too far in the future to worry about. But, at some stage, the argument will become of more than academic interest.

**Conclusions**

Although, as noted, the individual working groups frequently took positions that were at odds, it is possible to draw a few general conclusions:

- The Internet has great potential because it creates a new medium which is likely to be cheaper, more convenient and perhaps more fun to use than, say, the telephone or print.

- It threatens to revolutionize large swaths of the finance industry, though its influence will be most immediately felt at the retail end because:
  - it lends itself to distribution of fairly standard products to a mass market; and
  - the wholesale markets are more cautious about a medium that is still perceived of as relatively insecure and unreliable.

- Within the retail industry, some products are felt to be more amenable to Internet delivery than others—mainly the mass market, low margin products that require the least amount of human intervention. This could change over time, since the Internet also permits products to be “personalised” at relatively low cost. But, at the outset, there was broad agreement that the Internet would be a distribution medium for generic-type retail products and information.

- It was also agreed that the Internet poses a real threat to banks, intermediaries, insurance brokers etc. However, it also opens up new opportunities for banks:
  - to create new product variations for their traditional markets; and
  - to become suppliers of new products required by the Internet, e.g. electronic payment systems, and verification and authentication services.

- The Internet would benefit from the participation of banks in supplying these services. Greater participation by established financial service
providers would give the Net respectability and security, and would attract more users.

- At the moment, most banks are playing a watching game – “learning not earning”, with low level Web sites. They are treating the Internet as a parallel, not substitute, delivery channel, and virtually no new products have yet been specifically developed for the Internet.

- Growth of the Internet could well be held up by its lack of user-friendliness, by a lack of confidence among users, and/or by uncertain economics. All of these problems can be overcome – particularly the economic argument, since there is a lot of evidence that the cost of Internet transactions is only a fraction of the cost of “conventional” transactions. However, attention still needs to be given to these areas – perhaps at the expense of further technological sophistication.

- Security is also a problem, but there was agreement that this is less of a problem than generally thought. Encryption services are becoming increasingly available and banks may actually be able to supply the answer themselves.

- Regulation throws up difficulties. In the view of the working group, these are by no means insoluble – though it may be underestimating the task of obtaining international agreement. Whatever, clarification needs to be found in the areas of territoriality (whose rules apply?) and consumer protection, as well as concerning the legal status of electronic documents.

Finally, the working groups identified a number of contradictions about the Net that are worth flagging. Some are resolvable, but some go to its very essence:

- The Internet may be universal, but it is also anarchic (in the best sense of the term). No one owns it, or runs it, or sets the rules.

- Although it is Big News every day, much of what one hears about the Internet is hype from partis-pris Net-heads. Not much real business is being done on it yet, and not very many companies are making significant money from it.

- Although the Net is a new and open world, some of the most active users seem to be heading in the direction of closed user groups. Over the next few years, one of the main trends may well be to “fence off” parts of the Internet – a late 20th century enclosure movement.

- The Internet offers financial services providers two radically different options: they can mass market very cheaply their standard products, or they can use the Net to personalise their product range. In the short term, standardisation will prevail; in the longer run personalization will become more important.
The Internet and Financial Services

- The Net can be used to increase customer loyalty through customisation, etc. But the existence of software interfaces and the ability to shop around for the best deal may also increase the fickleness of customers, who will be able to change supplier at the click of a mouse.

- Most people expect the Internet to increase pressures on existing financial suppliers, many of whom can be disintermediated. However, it is equally the case that the complexity of the Net, and of the offerings on it, will require the growth of new specialities—financial intermediaries could take on a new role as interpreters of what is available on the Net.

- Although the Net denies geography (to the potential benefit of remote markets), it may also permit business from around the world to gravitate to traditional markets (the US, Europe) where best practices apply and where regulatory remedies are available. In that sense, business standards may level up, not down.
SECTION TWO: KEY FINANCIAL SECTORS

Chapter One: Retail banking

Summary: The Internet could be a "step change" for retail banks. Potential cost savings are enormous but that carries its own risk in terms of attracting new, non-traditional providers. The future needs banking; it doesn't necessarily need banks. The new players could be other trusted names - like supermarkets. They may be specialists (e.g. in the payments area) or card issuers, or even software houses. But banks have advantages - notably an existing client base, an image of integrity, a big investment in technology and an understanding of risk. So far, most European banks are still feeling their way - "learning, not earning" seems to be the motto. But, even if some early Net ventures have been disappointing, the demographics of the Net user are compelling and there is no sign that the banks are backing away from what could be a retail banking revolution.

Chairman: David Birch
Vice-chairman: Paul Taylor
Rapporteur: David Birch

Hyperion
Financial Times
Hyperion

Working group members:

Brian Allison
Julian Badcock
Tomás Carruthers
Martin Elton
Keith Gold
David Guest
Yoshitsugu Ichino
Alan Johnson
Jan Willem Kuenen
Tim Leslie
Michael Mather
Robin Rogers
Heather Rowe
Andrew Wood

PA Consulting Group
Ernst & Young
ESI
Andersen Consulting
IBM
Midland Bank
Dai-Ichi Kangyo Bank
Price Waterhouse
Edgar Dunn & Co.
SHL Systems
Bank of Scotland
Springman Tipper Campbell
Lovell White Durrant
BBC World Service

A representative of Morgan Stanley's banking team also participated in the group.
1. Introduction

The Internet is a communication channel, a distribution mechanism and a vehicle for electronic commerce. For UK retail banks, it also represents an opportunity to transform the business of banking. If they don’t take it, they could find their traditional franchise being eroded by non-bank institutions who see the relatively low entry cost of the Internet as an opportunity to muscle in on what has been a cozy, protected market.

Unusually, the idea of Internet banking is being led by consumers rather than being pushed by technology: individuals are signing up to the Net and looking for applications which justify their investment. Perhaps for the first time, retail banks face the prospect of customers demanding technological change in the form of Internet banking facilities, rather than seeking to impose change themselves.

But there is another reason why the Internet matters to banks. Unlike other technological changes, which have mainly involved automating manual operations, the Internet could actually change the core business of retail banking.

In this chapter, we attempt to assess the likely impact of the Internet on retail banking in the UK and suggest some of the strategies open to banks to meet the challenge. Among the main points:

- Consumers are signing up for the Internet in growing numbers, and they are accumulating experience of electronic commerce. The Internet is not, therefore, something that banks can ignore.

- Traditional banks face the possibility that, in an Internet environment, new entrants will ‘cherry pick’ their best customers.

- Banks that are prepared to pioneer the Net have the potential to attract new customers, though retaining them will be a challenge.

- Banks may repackage existing products for Internet delivery, but they will also need to develop new products for Internet customers if they are to win lasting market share.

- Banks have a unique opportunity to build a new business out of their ability to validate and authenticate parties to credit card transactions. But in order to obtain a significant share of the Internet retail payments market, banks will need strategies to handle micro and even nano-payments.

- Operating as a certification authority (or trusted third party) and providing other risk management services could eventually become a core business of Internet–based banks.

- Because of its interactive nature, the Internet could provide a way for banks to exploit their legacy systems, which are often described as inflexible or irrelevant. Supplying timely and valuable information could help banks build customer relationships on the Internet.
The Internet and Financial Services

- While it is difficult to quantify the size of the business opportunity it represents, bankers need to devote resources to understanding the Internet and to developing strategies for it.

Perhaps the most important conclusion of the working group is that it is hard to overstate the potential impact of the Internet on retail banking in the UK.

2. A step change for retail banks?

Consider the following statement and choose the more appropriate response:

“Internet banking is to retail banking as…”
- telephone banking is to branch banking;
- the eurodollar market is to the Federal Reserve.

If you chose (a), you probably believe that the Internet is just another technology that will not change retail banking in any fundamental way. If you chose (b), you may believe that the Internet marks an advance in technology that could transform retail banking. One can make a case either way. However, the sense of the working group – based on what has already happened in the US and what is beginning to happen in the UK – is that the odds favour radical rather than superficial change. We see change occurring in terms of:

- services offered;
- how those services are offered;
- who offers them; and
- to whom they are offered.

Some members of the global banking industry certainly believe that the development of the Internet is a major “step-level” change. For instance, John Reed, chairman of Citicorp, has said that over the next decade retail banking will become nothing more than “a line or two of code in a big network”. Even if it is not immediately clear what Reed meant by that, Citicorp evidently accepts that the future of retail banking will bear little relation to its past.

One important driver is clearly cost. The chart shows that the “virtual” bank can be much cheaper than its bricks and mortar equivalent.
Another driver is that the Internet has appeared, not as an isolated technological breakthrough but just one element of a broader information/communications revolution.

Recent IT developments – smart cards, network computers and so on – fit with the Net to link buyers and sellers in a "virtual market". The Internet does not, therefore, just mean a change in delivery channels; it is part of a shift in business models, which is much more difficult to plan for. Nor is its impact in the far-off future. The rapid increase in consumers with access either to the Internet or to commercial on-line services such as Compuserve and AOL means that there is already an electronic marketplace – even in the UK, where PC/Internet penetration is still far lower than in the US (though, as shown below, the PC market is precisely the one that is most attractive to suppliers of financial services). What is needed is the development of mechanisms to facilitate the transition to a truly "virtual marketplace" where trade is carried out with the same trust and confidence as in the physical marketplace.

---

**UK home PC purchases by household**

- Without Children: 57.7%

*Source: Computer Weekly/Kew Assoc. (August 1996)*

---

**UK home PC purchases by social grade**

- AB: 37.7%
- C1: 35.4%
- C2: 16.0%
- DE: 10.9%

*Source: Computer Weekly/Kew Assoc. (August 1996)*
The evolution of the Internet is still at a stage where the retail banking industry has the opportunity to take the strategic initiative. Despite their image, banks are no longer the "dinosaurs" described by Bill Gates; indeed, the UK finance sector as a whole now invests very heavily (by any standards) in information technology. Moreover, UK banks are aware of the Internet. In a survey by City Research Associates in August 1996,1 banks, building societies and finance houses said they viewed the Internet as the most important emerging technology. But while banks have already begun to develop an Internet presence, some in exciting ways, there is a gap between these early steps and having a fully-fledged strategy.

3. What the Internet could mean for retail banking

It is worth looking at what exactly is retail banking and how the Internet can affect each element. This is best done by viewing the business (a) as a process, and (b) as a set of functions.

The process

Retail banking involves:

- customer gathering and retention;
- service/sales; and
- service delivery.

It is clear that the Internet can play a role in each of these areas. But is this role really different from that played by other new technologies? In other words, what differentiates the Internet from technologies that have already been adopted by the banking consumer? Consider the two major technological changes which have affected retail banking over the last 25 years:

- The ATM has now become the main source of bank cash for individuals, though it has taken time for consumers to accept self-service, in spite of the obvious convenience. But essentially, the ATM has simply replaced a cashier with a mechanical operation; it has only changed the bank's relationship with its customers to a limited extent, though it has reduced the amount of personal contact between a customer and his bank.

- The growth of credit cards, on the other hand, has been more significant. Initially, control of them was limited to banks, but a combination of communications, magnetic stripes, image processing and, now, data warehousing has opened them up to new business categories. Other institutions such as AT&T, GE in the US and high street stores in the UK are seeking to build their own customer franchises directly. As a result, the high street banks' share of the credit card market is under pressure.

---

The Internet belongs to the second category: It should be viewed as a change in the process of banking that carries great opportunities. But it also implies a threat because it will attract new players into the business. It can also redefined the institutions used for retail banking. Initially, these new institutions will operate alongside more traditional banking, but the integration of the Internet with other technologies may well create new approaches for the financial services industry based on:

- **The ability to redefine customer franchises:** Typically, bank customers have shown little desire to switch banks—not least because it has been so difficult to do so. This could change, which would be good news for banks seeking to enlarge their market share. But the downside is that the Internet could enable institutions outside the financial services market to exploit their well-known brand names to reach new customers inside it. This is already happening in the UK with the move into retail banking by the supermarket giants.

- **The creation of new value chains:** New markets and new ways of transacting business may develop, making it much harder for banks to hang on to their business, particularly in the payments and asset financing areas. The Internet could also facilitate a return to customer intimacy (if customers want it) through highly specific interaction between bank and customer—potentially in real time. Products, pricing and communications can all be tailored to the needs of the individual; the question is whether it will be banks or their competitors who take the initiative.

- **A redefinition of organisational boundaries:** Organisations (including financial institutions) are already adopting distributed computing environments, with HTML technology allowing them to integrate business applications through widely-used and cost-effective standards. There are two effects:
  - a cultural change which stimulates individuals to develop new associations; and
• the potential to create new products and services by combining capabilities from many organisations.

• **A new foundation of trust between a bank and its customer:** This is an area where the banks' image of integrity stands them in good stead for the cyber-future. The growth of Internet business may be inhibited by the customer’s lack of confidence. The potential therefore exists for banks to take on an underwriting role – validating and authorising parties to transact business on the Internet – for a fee.

• **Markets becoming global:** The Internet does not recognise geographical boundaries. It therefore enables a financial institution to enter new geographical markets, probably at a lower cost than existing participants (subject, of course, to regulatory considerations). But this may not help the banks. Banks are highly regulated in all jurisdictions and, therefore, less well placed than their more lightly regulated competitors to take advantage of the Internet’s ability to open up new markets.

**The functions**

It has been observed that while the future needs banking, it doesn’t necessarily need banks. What is expected is that some form of organisation (bank or non-bank, regulated or otherwise) will provide:

• somewhere safe for people to hold their transaction balances;
• ways to make payments in order to facilitate trade;
• mechanisms for pooling resources to fund larger-scale enterprises;
• methods of managing risk; and
• price information, such as interest rates and securities.

How might the Internet affect these functions (and the products they imply) in the retail banking context?

**Transaction balances:** This is a tricky area. As the figure below shows, there is some evidence that, at least on a stand-alone basis, the traditional checking/current account is an extremely unprofitable product. If it is to be justified, it must be on the basis that it is required for cross-selling of other products.
Nevertheless, the Deloitte & Touche figures are derived from conventional banking. As we have already noted, “virtual” banking is a lot cheaper than bricks-and-mortar banking. Indeed, though the evidence is not yet in, it may well be that the low unit cost of an Internet-based system is the only way to make a checking account a profitable product in itself.

**Payments**: As discussed in another chapter, the Internet is already spurring innovation in this area – not necessarily to the advantage of the banks. For instance, the increasing use of advanced cryptography to provide simple and inexpensive payment systems could drive the margins on processing Internet payments down to the point where retail banks decide to leave it to specialists.

Paying bills is a good example. In a typical (non-Internet) home banking transaction today, the consumer issues an instruction via his PC or telephone which is processed by existing bank systems. In the future, when a consumer says “pay £20 to British Telecom”, his PC will go online via the Internet to his bank account and transfer £20 straight to the account of BT. In this case, banking networks would be bypassed completely, no settlement would be required, and the time during which value was out of interest-bearing accounts would be minimised.

Banks could also be cut out by cards. It is already clear that smart card-based electronic “purses” (such as Mondex, Visa Cash, Proton and Danmont) may come to dominate Internet payment. True, the assumption at present is that they will have to be charged up via a bank, but that is by no means inevitable. Indeed it may be more logical for supermarkets, which carry a huge float, to do the job instead.

Whatever, the range of payment services that could be offered to customers is wide, as shown in the figure below. This categorises payments by size and by when the payer loses interest on value – whether it is before the transaction takes place (as with a £5 note), at the time of the transaction (as with a debit card) or sometime after it (as with a cheque).
Where does the Internet fit into this continuum? We believe that it has a particular advantage in the area of small and medium payments:

- "Nanopayments" of less than £0.01, which are completely uneconomic at present, could become economic with a combination of the Internet, smart cards and e-cash.

- "Micropayments" of £0.01 to £10 are feasible but generally uneconomic through traditional banks. Firms like First Virtual have already developed competitive procedures utilising the Internet.

- "Minipayments" of £10 to £1,000, for which the Visa/Mastercard/Europay SET security protocol was specifically designed, are clearly profitable on the Net.

The Internet probably has little to add to traditional means of making "macropayments" (ie. over £1,000) in the foreseeable future, though with improved security there is no reason why it could not be used as a channel.

It is not technically necessary for these services to be offered over the Net by banks (in the US, non-bank specialists such as Cybercash have begun to do it). But if they can do so, they may expect a significant share of what could become a substantial payments market (with a turnover, according to an estimate by Forrester Research, of US$10bn a year by the turn of the century). However, a bank seeking a share of the Internet payments business will probably need to have a strategy to link micro and nano-payments with smart cards.

**Deposits and loans:** Banks have long had an advantage in attracting deposits, but it would be wrong to assume that this will continue to be the case in an Internet environment. Apart from bank-like alternatives — such as the UK’s First Direct (an offshoot of the Midland Bank) which offers most banking services over the telephone — consumers in the UK have already indicated
that they may be happy to deposit funds with a wide range of trusted institutions, including chain stores and supermarkets.

Banks do not have an exclusive franchise on trust. Consumers would clearly be happy to deposit their money with a number of different organisations. (Note that this poll took place before Tesco, Sainsbury et al. moved into retail financial services.)

So how can banks be sure of continuing to attract deposits in the new environment? One course of action is passive: post a schedule of interest rates/charges and wait for intelligent search engines to seek them out and bring in the business. The problem with this approach, however, is clear: relative to new entrants, full-service retail banks are likely to be high cost providers. Even if the Internet transforms the economics of the current/checking account, traditional banks will be at a competitive disadvantage and will, therefore, have to emphasise service and convenience to justify higher charges or lower savings rates.

Essentially, this means taking the branch into the customer’s house — not simply into, say, the supermarket. Assuming that advances in cryptography and smart cards enable the identification of a person sitting at a PC or TV to become routine, virtually all retail banking functions could be “outbanked”. The challenge is to transfer as much of a bank’s front office processing as possible on to the customer’s computer — and here the bank may have an advantage. It is the difference between a consumer filling out a form online and him downloading the “loan application” Java applet from the bank. In the latter case, the loan application is processed by the consumer’s PC, not the bank’s mainframe; only the results need to be processed centrally.¹

A further example might be a small business that collects cash payments on a Mondex card. Its point-of-sale (POS) terminal can be told to call up the bank and deposit the takings whenever they exceed £100. This terminal could be provided by the bank and could be integrated with the bank’s own systems — it would be an extension of the bank’s front office into the shop.

¹. Subject, of course, to regulations; e.g. the UK Consumer Credit Act still requires a regulated agreement to be in writing.
The Internet and Financial Services

Once customers have been acquired, managing Internet-based accounts is a potentially attractive business. Wells Fargo’s 300,000 online customers generate 90% fewer service calls than the average customer. This means that customer service resources can be cut back or re-focused on the remaining 10%. Since people no longer have to call up to check their balance – because they can do this on the Internet, and generally while they are at work – they only pick up the phone when they need significant advice. This opens the possibility of cross-selling other products.

But if consumers can arrange a personal loan on-line and automatically, why would they choose to go through a bank? Trust and reputation perhaps, plus the existence of a wider continuing relationship that non-bank competitors may not have built up (and may have little interest in building up). The banks can do a lot to foster this relationship – perhaps by personalising the service, for example by e-mailing customers when their account changes by more than a threshold amount, or when personal loan rates change. This develops an “account intimacy” which had become uneconomic in traditional branch-based banking because of the huge cost of transaction processing.

![Consumption of branch resources](image)

**Risk management**: Dealing with risk is already one of the core competencies of retail banks, and one that many non-bank competitors lack. In the opinion of the working group, the arrival of the Internet may well promote risk management to a dominant competency for banks in the networked economy.

Financial risk reduction – in the sense of insurance, diversification, hedging and so on – is just another financial service which can be translated to the world of the Internet, like mortgages and PEPS. But the Internet also throws up a new form of risk in the interaction of remote parties who want to do business in cyberspace. How does a customer know that he is really dealing with the retailer? Or, for that matter, with his bank? How can the retailer be sure about his customers? The infrastructure required to meet the security requirements raised by these questions is already under development – and it may well be an area in which retail banks have a major competitive advantage.
Legislation to enable the use of public key cryptography (discussed in more detail in Section 3) is falling into place and could provide a big opportunity for banks. The reason is that secure systems, based on cryptography, must involve at least three or four parties:

- a certification authority (CA) which can issue public key certificates;
- a certificate registry, (CR) where certificates issued by CAs may be scrutinised;
- a signing party – a person or organisation which uses a private key issued by a CA digitally to sign a message; and
- a relying party – a person or organisation which uses a public key obtained from a registry to check the signature on a message.

While the legal standing of digital signatures is still unclear in most of Europe, the Department of Trade and Industry (DTI) has issued a discussion document proposing a public key cryptography scheme for the UK. In this scheme, the CA/CR functions would be conflated into a Trusted Third Party (TTP) that would be licensed by the government – an approach that broadly corresponds with other European countries’ first steps towards digital signature legislation.

These businesses represent a real opportunity for banks:

- The CA business is ideal because banks have both physical presence and records. A bank would be able to issue a certificate and guarantee the identity of the holder because it can require the holder to come into a bank branch and provide physical identification.

- The CR business is ideal for banks because they have big databases with fast network access. They could store their own and other people’s certificates and make them available for a fee.

Plus, customers have confidence in banks. Not only do they have a reputation for integrity, they also tend to have deep pockets. If things go wrong, they are in a position to offer restitution – and if they don’t, they can be sued. (This is, of course, a reason why some banks may choose to stay out of this business.)

Banks’ back office computing resources might also be used to provide information within the certificate infrastructure. This might be as simple as a credit rating, but considerably more sophisticated possibilities can be envisaged. For instance, if a consumer needs to demonstrate to an on-line estate agent that he has a firm mortgage commitment from a bank, a digitally signed certificate would be the obvious mechanism.

But while banks would seem to have a natural advantage, they cannot afford to procrastinate. The US Postal Service, for instance, is soon to begin a variety of certificate services (as well as electronic postmarks for e-mail), and there are plenty of other organisations well-placed to follow suit, such as telephone companies and utilities.
Information: To provide any kind of service on the Net, a bank must be able to package (and organise) a range of useful financial and other information. Since the raw content is generally available on the Internet anyway, this means adding value to it in some way.

As the above chart shows, three-quarters of European bank Web sites still only provided information at a simple level in 1996 – perhaps because the prevalence of direct debits and standing orders means that there is less to be gained from more sophisticated sites with transactional capabilities. But technology offers the means to transmit information in a much enhanced form. For instance, a bank-provided F/X Java “bean” (a reusable software component that can be incorporated in PC software, TV set-top boxes, etc.) could become a standard part of some users’ desktops. A bank could then deliver chart data along with a charting applet, portfolio data with a portfolio manager and current account data with a current account analysis applet.

Consider the hypothetical example of a household contents insurance calculator: the consumer would input room sizes, contents, valuables and so on; the program would then use this to generate an insurance quote, while the bank’s back-office scoured news feeds, magazines on home furnishings, consumer electronics catalogues and on-line antiquities auctions for information about further items the householder might need.

Information is, of course, of greatest use when it enables people to make informed decisions. Its value would therefore be enhanced by including with it educational material to help customers understand it.

4. What is being done?
The previous discussion has been largely about the potential of the Internet. Few people in or close to the banking industry would deny that the Net has great potential, but what is actually out there? Is the retail banking industry seizing the opportunity? Or is it in danger of losing out to others – if, indeed, they are interested?
First, a few preliminary points from a 1996 survey of the Internet banking (covering both the US and Europe) by Booz, Allen:\footnote{Booz, Allen & Hamilton, op. cit}

- As of mid-1996 there were over 600 bank Web sites on the Internet – although, of these, three-quarters were just “electronic brochures”, with only 2% of European sites and 1% of US sites offering “full service” banking.

- The number of bank-sponsored Internet sites is growing very fast – about 90% a year in Europe and even faster in the US.

- Although US bankers are generally more aggressive about the potential impact of Internet banking, Europeans are no slouches – and, indeed, France and Germany (the two biggest European markets) have more experience than practically anyone else of on-line banking through Minitel and T-Online.

- In general, US bankers (who operate in a much more paper-intensive environment than in Europe) see the Internet more as a means of reducing transaction costs, while Europeans are focusing more on the delivery of high-value added advice.

**US: Who is setting the pace in the US?** Perhaps surprisingly, the answer is \textit{not Citibank}, the traditional market leader, which has said publicly that it will avoid a major commitment to Internet banking (unless its customers specifically request it) until it is happier with the security aspects. Instead, it is developing proprietary networks.

Among the 300 plus US banks that do have a presence on the Web, the one that has received most publicity is \textit{Security First Network Bank} (at http://www.sfnb.com) – which started life as a one-branch savings & loan in Lexington, Kentucky (though it is now owned by Cardinal Bankshares). This claims to have been the first Internet bank, operating since October 1995. Although its client base is still tiny – the \textit{Financial Times} said it had around 2,000 customers in September 1996 – the demographics of its customer base are very attractive. Security First is not alone; the Bank of St. Louis, Missouri, for instance has launched the Mark Twain Bank (using DigiCash technology and is located at http://www.marktwain.com).

But the pace of electronic banking has not been set by these banks or by similar ventures. At least 70% of home banking in the US (using Internet or private closed systems or intranets) is indirectly controlled by the software houses, and specifically by three popular financial management programs:

- **Intuit’s Quicken**: Quicken, which was introduced in the late 1980s, is installed on about 10m PCs in the US. In mid-1996, Intuit introduced a new home banking package through AOL, the Internet service provider, which enables customers of the three dozen or so banks that use Quicken (Wells Fargo is one of the best known) to do most of their routine banking
transactions from home. Intuit is also working with Fidelity to open up the fund management area.

- **Microsoft’s Money**: This is used by around one million PC users in the US, and can also provide bank-backed home banking services. In mid-1996, it announced a complete bill-paying system in co-operation with Visa.

- **Meca Software’s Managing Your Money**: This has about half a million installations in the US.

There are plenty of other software houses moving into this field. In March 1997, for instance, Digital Insight (which specialises in providing Net-based home banking for credit unions and community banks) claimed 27,000 households were hooked up to its AXIS Home Banking System — with 3,000 new accounts joining every month.

It is clear that US banks are worried about this invasion by software houses. Even though Quicken is just a way to bring your bank to your house (and is not a bank itself), it is now very easy for Intuit to let its customers browse through the details on offer at any of the banks whose services it carries. The danger is that the customer becomes more familiar with the interface than with the bank and could ultimately stop caring who conducts his financial transactions. That could be devastating to customer loyalty and to the possibility of cross-selling by banks.

For many banks in the US, the lead that the software packages have established in this area may already be too great to claw back. But, in September 1996, 15 banks (led by BancOne, NationsBank, BankAmerica, First Chicago NBD, Mellon and Barnett, and including the US operations of ABN Amro) hooked up with IBM to offer their own financial interface, to be known as Integrion. This is an important initiative since it represents the first time that banks have co-operated to fight back. It will apparently be offered both through the Internet and, if customers demand it, through IBM’s own private network. The advantage to the banks is clear: they will continue to control their own branding; no other provider will be interposed between them and their customer base.

Now, attention is focused on Citibank and Chase Manhattan, the two giants of the New York banking scene. So far, both have said they will concentrate on proprietary systems, but recent breakthroughs in cryptography could change that by opening up the Internet to secure transactions.

**Europe**: As the Booz, Allen study pointed out, this is not an area where the UK — usually the most innovative of European markets — really stands out. As shown below, there are more bank Web sites in Germany and Italy than there are in the UK. (Although these figures may be a bit out of date, we believe the ranking is still pretty accurate)
<table>
<thead>
<tr>
<th>Country</th>
<th>Number of bank Web sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>28</td>
</tr>
<tr>
<td>Italy</td>
<td>17</td>
</tr>
<tr>
<td>UK</td>
<td>16</td>
</tr>
<tr>
<td>Austria</td>
<td>14</td>
</tr>
<tr>
<td>Benelux</td>
<td>13</td>
</tr>
<tr>
<td>France</td>
<td>13</td>
</tr>
<tr>
<td>Eastern Europe</td>
<td>12</td>
</tr>
<tr>
<td>Scandinavia</td>
<td>10</td>
</tr>
<tr>
<td>Spain</td>
<td>8</td>
</tr>
<tr>
<td>Switzerland</td>
<td>8</td>
</tr>
<tr>
<td>Ireland</td>
<td>5</td>
</tr>
<tr>
<td>Greece</td>
<td>4</td>
</tr>
<tr>
<td>Other</td>
<td>7</td>
</tr>
</tbody>
</table>

*Source: Booz, Allen & Hamilton*

Moreover, France and Germany have a longer experience of on-line banking than the UK:

- France has 15m Minitel users who can access bank accounts and make bill payments.
- Germany has 3,000 financial institutions who offer full banking services to 1.2m T-Online subscribers.

The problem is that the existence of these networks may well inhibit Internet take-up. Why bother to use the Internet, even if it can do more, when these systems are already up and running? There are exceptions: Credit Mutuel de Bretagne, for instance, has offered Internet access since September 1995 via its own secure Citelis service. This is, in theory at least, twenty times as fast as Minitel, and can be hooked into money management programmes like Quicken, but the take-up has so far not been impressive. Plus, France Telecom is offering Wanadoo, an on-line package which allows Internet access as well as Minitel. But, on the whole, the sunk investment in Minitel will hold the Internet back in France.

The UK does not suffer from this handicap. True, the Bank of Scotland has offered its own Home Office Banking Service (HOBs) since 1985 but this is essentially a dedicated private network service that has only recently been re-engineered to permit access via PC and modem. (Originally, access was via Prestel, then through Minitel terminals.) Although it, too, now offers HOBs for Windows, with a hook-up to Money or Quicken, it is not yet an Internet product.

The UK bank that has probably gone the furthest in the direction of Internet connectivity is Barclays, which set up Barclaysquare – an Internet shopping mall joint venture with Netscape and Interactive Telephony – in May 1995. Customers of Barclaysquare can shop for a variety of goods and services (including Eurostar tickets) using their Barclaycard (Visa) as payment, reinforced by Netscape encryption. The avowed philosophy of this venture was to “learn not earn”, and it has undoubtedly taught Barclays a lot. But there are doubts in
the industry over quite how successful it has been, either as a banking or a retailing venture, and its creator, the American Joseph de Feo, has moved on. Barclays has now gone one step further and is offering all its customers an on-line banking system as a joint venture with Microsoft. Surprisingly, there have also been reports that the system might eventually link up with Intuit as well, so that Quicken can be incorporated.

Most of the other UK clearers are still some way behind Barclays. Nevertheless, they are heading in the same direction and one or two are catching up fast. For instance:

- **NatWest**: Following the BarclaySquare model, NatWest has set up its own Buckingham Gate mall with ICL and Netscape, offering up-scale retailers and a variety of payment options (including Mondex). In parallel, it has been running a small Internet-compatible PC banking service since November 1995.

- **Lloyds TSB**: TSB has been one of the more innovative UK banks in this area. In May 1996, it linked up with Compuserve to offer an on-line service to Compuserve subscribers for which it provided free software. As of January 1997, around 12,000 had applied for the service, of which (it is said) 25% were new customers.

- **Royal Bank of Scotland**: The most recent new entrant is RBS. In late January 1997, it announced what it claimed to be the first full service Internet bank in the UK, employing enhanced cryptography and underwritten by an RBS guarantee of a transaction’s integrity. This service is offered through Microsoft and will be marketed aggressively.

At a different level, **Secure Trust**—a small banking and personal finance group—also offers direct access to its banking services via the Net.

The Antigua-based **European Union Bank** achieved a degree of notoriety in 1996 by soliciting for banking business in the UK—thereby attracting the attention of the Bank of England. But, in general, there is still a long way to go before cyberbanking takes over in the UK.

**5. Where next?**

The growth of Internet banking is a classic example of the so-called “network effect”—the very presence of retail banks on the Internet helps to legitimise its use by individuals and businesses. This means that banks have an ability to stimulate other on-line business and to attract new customers for their own banking services.

The most promising market segments in this regard are small and medium-sized businesses and individuals who can see the benefits of trading on-line but need reassurance before they will start. This is where the **bank-run ‘shopping mall’ model** might still provide value.

Clearly, national retailers with their own brands do not necessarily benefit from being in a bank mall. Smaller retailers are different. One strategy for
retail banks is, therefore, to provide malls for their personal and small business customers. Rabobank, a big mutually-owned institution in The Netherlands, has begun to develop this kind of service, with a strong local focus. This kind of approach solves two problems simultaneously:

- “selling” customers have an incentive to do business on-line because the bank is shielding them from complexity; and
- “buying” customers feel more confident because the bank is, in some sense, testifying to the soundness of the vendors simply by giving them space in the mall.

Agreements between banks to link up their malls would help to stimulate this sort of activity, in the same way that ATM reciprocity has done.

Another way of dealing with consumer wariness of the Internet is through guarantees. The US’s third largest card issuer, AT&T, has promised to indemnify anyone who is defrauded while using its Universal credit card over Worldnet (AT&T’s Internet service provider).

Banks will also have to do more to identify which customers might best be attracted to Internet banking. Here, the enormous data banks that they have developed ought to give them a huge competitive advantage over newer entrants. They may choose to reinforce this by differential pricing (i.e. using product pricing to attract desirable business to the Net), though this also runs the risk of alienating existing customers.

Retail banks might consider providing an Internet presence (and Internet transaction services, where appropriate) as part of their standard offering to small business customers. It is these small and medium-scale enterprises that would most benefit from expanding their customer base through this new, inexpensive channel, but they often lack the expertise and the confidence to get on-line.

6. The hurdles

While the Internet holds out enormous commercial possibilities, the way forward is also fraught with risk and uncertainty. Despite the experience of the last few years, there is no definitive answer to the key questions bankers tend to ask:

- Can banks make money from the Internet?
- Does the Internet open up new markets or merely cannibalise existing ones?
- If new markets do exist, are they big enough to make any difference to bank strategy in the foreseeable future?
- Will cyberspace end up as over-banked as the UK is now alleged to be?

The economics: Most of the major UK banks have been criticised for their apparently sluggish response to the Internet. But, like any business, they have to be convinced that it is worth the investment. Forrester Research, in 1996, calculated that an Internet site providing full banking functions would cost in
the region of US$3.4m to set up. Even a site with limited interactivity would cost around US$300,000. These are not huge amounts, but they are significant—and, of course, once up-and-running, a site must be maintained and serviced and, where interactivity is involved, that can be expensive in both cash and executive time.

Against figures like these, where is the income in cyberspace for banks?

Few, if any, UK banks have managed to answer that question. Even Barclays, in some respects the leader in the field, has acknowledged that it sees Barclaysquare as a loss leader; NatWest appears to have adopted a similar strategy with Buckingham Gate. The lack of firm information on the number of Internet users is another stumbling block. The UK figure could be anywhere between 300,000 and 3m—a huge margin when investment decisions have to be made.

However, it is already clear that the economics of the Internet are very different to those of the conventional financial service provider. Banks with sufficient computing capacity that can regard their start-up expenditure as a sunk cost might earn tremendous profits from bringing new customers on board. Transaction processing costs are also many times lower than for those conducted via a branch network. It is estimated by Booz, Allen, for instance, that the ratio of costs to income for an Internet bank is 15-20 per cent, compared to a traditional industry figure of 50-60 per cent.1 This suggests that the Internet should be able to sustain a larger number of banking entrants, but that competition for online business will be commensurately fiercer.

<table>
<thead>
<tr>
<th>Retail banking unit transaction costs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Branch</td>
</tr>
<tr>
<td>Phone</td>
</tr>
<tr>
<td>PC</td>
</tr>
<tr>
<td>Internet</td>
</tr>
</tbody>
</table>

Source: Booz Allen & Hamilton (1996)

Traditional banks should be well-placed to fight a prolonged price war. But they face the additional threat that new entrants may use the Internet to “cherry pick” the best products and markets, while avoiding low value transactions. This could accelerate the transition to Internet banking in two ways: by attracting the better banking customers to the Internet, and by reducing the profits available

to traditional banks to cross-subsidise their branch networks. But this also means that banks with a well-developed Internet presence should be able to rationalise their branch networks more quickly than those without. They will also be better placed to lock in their most desirable customers.

**Consumer resistance:** The more radical advocates of the Internet argue that cyber-banking will eventually lead all consumers down the road to digital Nirvana. Banks as we know them will become nothing more than a memory. However, it is worth remembering that most bank customers are extremely conservative. Take the example of the US: credit cards, debit cards and ATMs were confidently expected to decimate the cheque business; in fact, 50-60 billion cheques continue to be written each year, which suggests that claims about the inevitability of technology should be treated with caution. Despite all the talk of the Internet “breaking down barriers”, the majority of UK consumers are likely to favour brands they know and trust – though not necessarily traditional banking names. Nor can the Internet yet provide the level of mass market user friendliness required for rapid and sustained growth in home banking. However, with the growing acceptance of PCs in the home and the growth of ‘money management’ software, this may not remain the case for long.

Initially, Internet banking will therefore tend to appeal only to the technologically and financially sophisticated. If it is to reach a wider market, it must offer something new and compelling: a capability that traditional banking cannot offer (for example, the ability to transfer bank account details or stock portfolios straight into one’s own financial analysis packages).

This resistance suggests that, for the time being, banks will concentrate on learning – marketing their Internet services to complement existing distribution channels rather than to replace them. It may be a matter of repackaging existing lines for the Internet, and using the branch as a sales outlet for value-added services where personal interaction is required. However, those banks which emerge as the Internet leaders will learn a lot about their customers and may soon come to the view that the Internet offers much more powerful possibilities. They will then proceed to the next strategic stage – creating new products specifically for the Internet customer.

Once the Internet gains wider acceptance, banks will face a new challenge: highly mobile customers, who will be able to change their Internet bank at a key stroke. Since profitability varies greatly across customer segments, this will require banks to be continually creative – implementing new products with a focus on customer retention. **Usability will be a major factor:** no one will battle through a difficult Web site (or one that is slowed down by unnecessary graphics) to buy a financial product.

**Regulation:** A number of regulatory and legal issues also have to be resolved before UK banks go full-speed into cyberspace. Many of these have to do
The Internet and Financial Services

with the regulatory status of financial information supplied over the Internet, and territoriality. They are discussed in detail in Section 3.

7. Conclusion

While hurdles to progress exist, the Internet is a potentially momentous development for retail banking. In the view of the group, the priorities for UK banks at this stage should be to focus sufficient resources on the Internet to:

- gain experience;
- build up brand awareness as an Internet innovator;
- be well-positioned to react quickly to Internet developments;
- learn how to add value to transactions, be they card-based or part of an ‘electronic purse’;
- tailor Internet products and services to meet the requirements of specific categories of customers;
- build on the expertise they already have for providing a secure environment for the transmission of financial data;
- position themselves as validators of Internet traffic;
- use the Internet as a means of gathering useful information on consumers so as to develop specific new products;
- adopt a phased approach to on-going Internet developments, recognising that it is a technology which will evolve as time goes on; and
- form strategic partnerships where they can add value to the payments process for virtual trade.

In other words, the Internet is not something susceptible to the normal kind of “five-year planning” that retail banks have tended to go in for. The key is knowledge, flexibility and fluidity, so that different scenarios can be sketched out and so that the organisation can build in the ability to change quickly and to respond pro-actively to the evolution of the Internet and to the activity of competitors.
SECTION TWO: KEY FINANCIAL SECTORS

Chapter Two: Personal finance

Summary: Personal finance is a huge and amorphous area, but it is one in which the Internet could make an enormous difference. Initially, this will probably be at the "commodity" and information end, where price rules. But, in the longer term, the Net may also lend itself to the marketing of more complex, personalised financial products. Already, many financial service providers are establishing a Web presence and an increasing number are genuinely interactive. As this number increases, a key issue will be navigating around the Web, whether through intelligent search engines or via increasingly comprehensive link pages. At present, the Web has a lot to learn in terms of simplifying the user's life but huge strides are being made - to the ultimate benefit of the financial consumer. But, if he wins, who loses? Probably the IFAs are the most at risk - though they could also be big winners if they were able to take full advantage of the Net, perhaps even becoming personal guides to the potential of the Web.

Chairman: Alan Brener
Vice-chairman: Arnold Dreuth
Rapporteur: Alan Brener

Business Technology Network

Working group members:

Antony Aitken
Stephen Aitken
Julian Babcock
John Bonham
Tomás Carruthers
Nick Collin
Sarah Denby-Jones
Mark Hayes-Newington
Christopher Hildrich
John Lancashire
David Stewart
Richard Stones
Alan Sully
Daniel Tunkel
Justin Urquhart Stewart
Joachim Utans
Andrew Wood

Transition Partnerships
DTI Innovation Unit
Ernst & Young
Linklaters & Paines
ESI
SRI International
PFour Consulting
The Research Department
Simmons & Simmons
Bacon & Woodrow
McGurn Stewart & Partners Ltd
Lovell White Durrant
Sun Life
Barclays Stockbrokers
London Business School
BBC World Service

The group included other members who have requested that their names not be used.
1. Introduction

If the Internet is to play a part in personal finance it will, in words that have become a cliché, be through “the empowerment of the customer”.

In a radical scenario, the Internet could remove the need for intermediaries between the individual and his financial objectives. Consumers would take charge of their own financial destinies: national boundaries would evaporate, distinctions between financial products (mostly invented by financial institutions anyway) would disappear, followed in short order by branch offices, administrative centres and wads of marketing literature. In an Internet world, barriers to entry would be swept away, allowing new firms to move in with innovative techniques. In no time, investors – even the relatively unsophisticated – would have access to all the information and services they need to manage their own financial affairs.

The result could be that a customer, using only his television set, would obtain his pension from a firm in Iowa, buy a German bond and invest in a tax-exempt scheme put together in Dublin. All this could be achieved with the help of an “intelligent” search agent and a fairly standard financial software program.

But will it happen? Or will the Internet turn out to be more sizzle than steak?

This chapter examines the extent to which this vision of an Internet future could be translated into reality in the personal finance area and the effect it would have on present-day providers. It will also propose ways in which intermediaries might rise to meet the challenge.

2. Who uses the Internet?

The Internet has spawned a mass of contradictory information. Many reports speak of brave new worlds. But a 1996 analysis of investment prospects for the Internet stated that fewer than 300,000 UK residents who own a personal computer at present have an account with an Internet Service Provider or regularly access a bulletin board service. The biggest user group comprises middle class males aged 25-34, and the most popular Internet content is erotica. According to the report, only 12% of UK users have made a purchase over the Internet, mostly for computer-related products. A more recent US study by Neilson Media makes the same point: only 15% of regular Internet users have ever made a purchase over the Net.

Is this pessimism justified, or are those who foresee a US$600bn Internet market by the year 2000 right? As the chart below indicates, a strong case can be made either way:

---

1. Diefencher, op. cit.
The Internet and Financial Services

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low entry cost and rapid technical development</td>
<td>but Too many players and consumer confusion</td>
</tr>
<tr>
<td>Lower cost of telephone calls</td>
<td>but Current calls still too expensive (in the UK)</td>
</tr>
<tr>
<td>New user-friendly delivery channels</td>
<td>but Compelling delivery channels</td>
</tr>
<tr>
<td>Improved intelligent agents</td>
<td>but Poor access</td>
</tr>
<tr>
<td>Security concerns being met</td>
<td>but Perception of poor security</td>
</tr>
<tr>
<td>Increased consumer interest and IT skills</td>
<td>but Technophobia and small user base</td>
</tr>
<tr>
<td>Regulatory holes</td>
<td>but Legal uncertainties</td>
</tr>
</tbody>
</table>

One reason for these contradictions is that the evolution of the Internet is not a smooth process but a (relatively) slow progression punctuated by sudden leaps. The slow phase occurs while solutions to a problem are being tried out. The leap comes when a new technology is adopted as a standard. This pattern applies to most Internet-related applications, including those in areas like home banking and portfolio management.

**In the short term, what is likely to happen?**

The working group looked at user attitudes to the Internet and found four distinct groups:

- **The regular user** who logs on to the Internet every day at work to receive and send information relating to his job and outside interests. He also has Internet access at home.
- **The occasional user** who logs on to the Internet once in a while and can navigate the Web comfortably with a browser.
- **The consumer who has not yet used the Internet**, but is beginning to think he should.
- **The individual who is unlikely ever to use the Internet.**

**Regular users**: These could be described as “self-supporting” since they have the knowledge, skills and contacts to make their own financial decisions. They are likely to make extensive use of software such as personal management packages, intelligent agents and comparative databases. They probably show little loyalty to a specific financial service provider and will tend to seek out the best value for money. They expect information and systems to be available 24 hours a day. They also expect quick responses, strong security and a regular exchange of information with those whose services and products they are using. They probably renew their computer systems every couple of years.

**Occasional users**: These tend to rely on traditional sources of financial information (e.g. paper publications) but they might use execution-only services on the Internet, especially if these were linked to ready means of payment like their bank accounts. They might also try out a personal financial software
package like Quicken or Microsoft Money. In general, they would probably rely on their banks or brokers to come up with branded investment services, though they might see other providers — such as retailers or telecoms companies — as reliable suppliers too. This class of consumer is likely to expand because it will include a growing number of retirees as the technologically adept generation advances into old age.

The number of individuals in these “active” categories presently appears to be small. Consequently, it is unlikely that there will be a mass market for financial services via the Internet in the next few years — at least until access becomes easy and inexpensive. Nor is the arrival of additional financial products and services on the Internet likely to draw in much new business since these will almost certainly be copies of what is available through more traditional means. It is possible that a wholly new Internet service or application might be developed which could transform the market, as the spreadsheet did for personal computers. But nothing currently indicates that this is likely to happen. Another possibility is that new services could evolve which are only possible through the Internet. But at present most financial institutions view the Internet as an alternative rather than a primary marketing vehicle, and are putting little effort into Web-specific product innovation.

Nevertheless, several factors might help to create a mass market on the Internet. In particular:

- increased inter-connectivity of offerings (e.g. completely automated shopping, billing, portfolio management, etc.);
- availability of the Internet via existing television sets;
- widespread and cost-effective video-conferencing services to facilitate face-to-face consultation; and
- a steady reduction in costs for both service providers and consumers (and a transfer of some costs to the consumer, who is now able to take on some of the service provider’s back office function through his own computer).

<table>
<thead>
<tr>
<th>The “Interactive Investor” site</th>
</tr>
</thead>
</table>
| This free site — at http://www.iil.co.uk — aims to be a one-stop personal finance site for UK investors. It covers PEPs, unit trusts, investment trusts, pensions, offshore investments, insurance, mortgages, etc. (including performance histories of some 15,000 investment vehicles world-wide) and offers services from major providers such as GAM, Gartmore, M&G, Standard Life, Flemings, Schroders and Prolific. Application forms are available on-line, along with:

- **A finance directory**: A guide to UK and non-UK financial services companies.
- **A business monitor**: International professional and business intelligence.
- **Find an IFA**: A register of over 6,000 IFAs.
- **News**: From a selection of financial publications (including several FT magazines).
- **A jobs register**: Specialising in finance related positions.

Once a user registers — which is quick and free — a portfolio can be created and automatically monitored. The service is linked to the Association of Unit Trusts and Investment Funds, and the Association of Investment Trust Companies. |
3. The financial services spectrum

There are many definitions of the personal finance sector. For the purposes of this chapter, the working group chose a fairly wide one which includes personal loans, mortgages and bank accounts (current, savings etc.).

The group tried to assess the extent to which different types of financial product might be suited for sale through the Internet. The left hand side of the chart below lists some of the products which are thought to be most amenable to Internet distribution, i.e. those where supply can be automated and where price is the primary issue. These include information provision and commodity products. The right hand side lists the more complex products and services, including portfolio management and pensions, which require more personalised delivery. This second group offers the greater profit margins, but is also the more difficult to market on the Internet. In between, the chart points to a range of products which might strike a balance between these two extremes: execution-only dealing, mortgages and various savings schemes. At least in the short term, the Internet is likely to have the effect of shifting the market to the left of the spectrum by encouraging the standardisation of products such as pensions and personal savings, so that they can be marketed electronically.

It is also helpful to think of products in two broad groups:

- those which are actively required by the consumer (e.g. bank accounts, life insurance to support a loan or mortgage, etc.); and

- discretionary purchases, such as savings and insurance products.

The marketing emphasis of the first would be on service, of the second on value.

4. Setting up and managing a personal finance Web site

Broadly, there are three types of financial services site:

- **Own site**: This is by far the most common, used both by product providers and independent financial advisers. There are now surprisingly cheap models available that can be customised, though most such sites are still outsourced.

- **Host site**: For example, Virgin Direct initially started as part of the Condé Nast publishing site.
Multi-user site: The pioneers in the UK were NatWest's Buckingham Gate and Barclays' BarclaySquare - both of which are "landlords" to a number of merchants, including Sainsbury, Eurostar, Austin Reed, etc. More relevant, however, may be the financial sites run by MoneyWorld and Interactive Investor or the US's Investorama site.

Most of the sites provide information in the form of mixed text and graphics, setting out services and products.

The multi-user site may be the most attractive way forward for financial service firms (at least, at the beginning) because it allows them to concentrate on marketing while the host manages the infrastructure. Like an ordinary high street, such a site attracts shoppers, simplifies choice for them, and provides a measure of comfort. Leasing space on these sites is a low-risk, low-cost way of piloting an Internet presence. The disadvantage is that a multi-user site facilitates comparison between the firms and services offered. The benefits, however, probably outweigh these concerns.

A straw poll was carried out by one member of the working group into the attitudes of several product and service providers:

- Most of the firms with Web sites said that they did not expect much new business from their Internet presence.
- They believed, however, that they needed a Web site to improve their expertise in this field.
- They felt that future development was unpredictable; but the Net was one possible distribution channel which needed to be covered.
- The general feeling was that if their competitors were on the Net, they should be there too.

It is not clear how often sites are serviced to bring them up-to-date. This is an important function which some companies tend to overlook. A number of companies have also allowed different business divisions to set up their own sites without much thought about common standards or cross referencing. Other firms have adopted a house Internet style, much as in other media.

At present, few firms conduct financial transactions with their clients directly over the Net. Where they do, they tend to be in the US rather than Europe or Asia. What is perhaps surprising, given the low cost of entry, is how few small firms are represented. This may reflect their aversion to risk, their unwillingness to bear the maintenance costs of a good site, or simply lack of familiarity.
UK financial sector Internet offerings: A survey of some UK financial Web sites was conducted by the group in September 1996. These were rated on a number of criteria:

- **Ease of access**: How easy to locate it and links to the site.
- **Server speed**: How quickly the page loaded and how fast interactivity was.
- **First Impressions**: Evaluation of the general design of the site and how easy it was to navigate.
- **Content**: Quality of graphics, how useful the links were, how often it is maintained, etc.
- **Interactivity**: How responsive to the user and the possibility of sending emails.
- **Unique features**: Did the site offer anything distinctive or any compelling reason to return?
- **Overall impressions**: Was it a proactive or reactive effort on the part of the company?

Each of the sites was given a score of one to five:

- **One**: A limited attempt at Web site development. Poor information content and/or lack of maintenance.
- **Two**: Basic understanding of HTML use and Net capabilities.
- **Three**: Good use of HTML with good information content but limited interactivity.
- **Four**: Attractive site, displaying a wide range of services including interactivity. Well-maintained and information.
- **Five**: Innovative and among the best. Very easy to use with a good balance of graphics and text. Maintained with frequent updates, announcements of forthcoming attractions, etc.

<table>
<thead>
<tr>
<th>Company</th>
<th>Address</th>
<th>Overall assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearl Assurance</td>
<td><a href="http://www.pearl.co.uk/pearl/">http://www.pearl.co.uk/pearl/</a></td>
<td>1</td>
</tr>
<tr>
<td>Northern Rock</td>
<td><a href="http://www.nrock.co.uk">http://www.nrock.co.uk</a></td>
<td>2</td>
</tr>
<tr>
<td>Royal Bank of Scotland</td>
<td><a href="http://www.royalbankscot.co.uk/home.htm">http://www.royalbankscot.co.uk/home.htm</a></td>
<td>3</td>
</tr>
<tr>
<td>Bank of Scotland</td>
<td><a href="http://www.bankofscotland.co.uk/home.html">http://www.bankofscotland.co.uk/home.html</a></td>
<td>3</td>
</tr>
<tr>
<td>Barclays Bank</td>
<td><a href="http://www.barclays.co.uk">http://www.barclays.co.uk</a></td>
<td>4</td>
</tr>
<tr>
<td>Nationwide</td>
<td><a href="http://www.nationwide.co.uk/homepage/homepage.html">http://www.nationwide.co.uk/homepage/homepage.html</a></td>
<td>4</td>
</tr>
<tr>
<td>Norwich Union</td>
<td><a href="http://www.norwich-union.co.uk">http://www.norwich-union.co.uk</a></td>
<td>4.5</td>
</tr>
</tbody>
</table>

As in the physical world, managing multiple brands presents problems on the Internet. Strength in individual geographical markets often requires a clear branding strategy. A good example is the retention by the National Australia Group of its three strong regional banking brands in the UK: the Clydesdale, Northern and Yorkshire. The same is true in cyberspace. Already, Northern Bank has two Net identities: one for its main business, the other for its offshore products. This is a logical split given the different target customers.

A number of lessons may be drawn in establishing and managing a Web site:

- The initial cost for a very basic Web site is around £15,000. However, it is not uncommon for major financial institutions to spend well over £50,000 designing and implementing an information-only site.
• At least six weeks should be allowed for the design stage alone.

• Too complex a Web site can result in slow downloading, perhaps to the point of causing a loss of interest and, consequently, the loss of a potential client.

• As with any communication with consumers, consistency should be maintained between offerings by different parts of the company.

• Links should be included between sites; Net addresses should appear in printed material, and postal addresses and telephone numbers should be placed on Web sites.

• The best sites offer something useful to the user, beyond information about the company products – preferably something that requires return visits: e.g. updated product comparisons and/or forms of entertainment.

• Once established, Web sites must be maintained and improved. This requires a long-term commitment. Having a Web presence is a process, not a one-off investment.

• Comparisons with competitors should be made frequently, including browsing their Web sites. It may also be useful to look at the sites of companies in other business sectors.

• To establish the value of the site, customers should be tracked and given a chance to make suggestions by e-mail about what they would like to see. The site should be used as a source of business information, e.g. the volume of sales generated, the conversion rate, etc. (This is now possible with Java technology, but there are important legal and privacy issues involved in building up user profiles in this way.)

• Links from other sites to the Web page should be encouraged. The more links lead to a site, the more likely it is that users will have a look.

5. Current offerings

Internet sites by financial institutions can be broken down into four main categories:

• **Marketing sites**: In these, a company uses its Internet presence to disseminate information about itself. It may offer links to related pages, or provide an e-mail address for inquiries. It is generally a “passive” site in that it only gives information, rather than receiving it as well. It may allow users to ask for specific information to be sent to them, thereby requiring them to enter personal mailing details, but little else.

• **Interactive sites**: These Web pages ask for specific feedback from the user or offer follow-up services. To achieve interaction, some form of basic service (like access to one’s bank account or investment portfolio) is required. Generally, these pages provide this sort of access free, or as part of a wider agreement between the user and the service provider.
The Internet and Financial Services

- **Service sites:** These provide a specific service via the Internet — for instance, the ability to make direct payment orders from one’s bank account. Through the Internet, the firm provides the user with a more efficient service than is otherwise available.

- **Advanced service sites:** These offer services not otherwise possible. Usually, they require the firm to enter into partnership with other providers of financial or auxiliary services — for example, to supply a personal finance system which allows the user to manage his bank account and investments, make payments, or even go shopping.

At present, most UK financial service companies see the Internet principally as a way of displaying their wares at a low cost. However, reduced costs are also a draw for new competition. Perhaps it is these new entrants — with little to lose and no legacy systems to hinder them — who will spur the growth of financial services on the Internet. That said, established financial institutions still have an edge. Companies with high-quality brand names like the Halifax, Allied Dunbar, HSBC/Midland, Barclays and NatWest are the standard bearers of the UK’s financial service sector Web presence.

---

... and some non-UK financial sector Internet offerings

Continuing the assessment made in the preceding box, here are the results for some non-UK sites:

<table>
<thead>
<tr>
<th>Company</th>
<th>Net address</th>
<th>Overall assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salem Five</td>
<td><a href="http://www.solemfive.com">http://www.solemfive.com</a></td>
<td>3.5</td>
</tr>
<tr>
<td>Fidelity</td>
<td><a href="http://www.fid-inv.com/index.html">http://www.fid-inv.com/index.html</a></td>
<td>3.5</td>
</tr>
<tr>
<td>(principally due to slowness, else 4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apollo Trust Company</td>
<td><a href="http://bankswith.apollotrust.com">http://bankswith.apollotrust.com</a></td>
<td>4</td>
</tr>
<tr>
<td>Toronto Dominion</td>
<td><a href="http://www.tdbank.ca">http://www.tdbank.ca</a></td>
<td>4</td>
</tr>
<tr>
<td>Bank</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BankAmerica</td>
<td><a href="http://www.bankamerica.com">http://www.bankamerica.com</a></td>
<td>5</td>
</tr>
<tr>
<td>Wells Fargo</td>
<td><a href="http://www.wellsfargo.com">http://www.wellsfargo.com</a></td>
<td>5</td>
</tr>
</tbody>
</table>

In general, non-UK sites tend to score better. As the Internet places all firms on an equal footing, this suggests that UK firms should improve their presence on the Web.

But there are others. MoneyWorld (http://moneyworld.co.uk) offers access to numerous UK financial sites on the Net, including building societies, life insurance companies and unit trusts. MoneyWorld has also launched a site providing a guide to ethical investment, sponsored by Friends Provident. This was the UK’s first attempt at a coherent financial Web-link service, though a similar service is now being offered by Omnium Communications Limited under the FIND label (http://www.find.co.uk). This service takes advertisements from financial companies, divides them into service categories (banking, mortgages, etc.) and provides quick links to them. However, being an advertising service, it only carries information on companies which have paid to be there. In the US, Investorama (http://www.investorama.com) is increasingly becoming
the major personal finance page, offering quotes, information and managed funds, as well as a host of news and related financial information and contacts.

Mention should also be made of financial software packages, such as Quicken and Microsoft Money which help people manage their personal financial affairs: bank accounts, investments, tax etc. It is not uncommon (in the US, at least) for these packages to connect directly to banks, thus providing users with a complete “front-end” to their bank accounts. This is significant because the customer may become tied to the interface rather than to any particular financial service provider. The software house could, thus, come to control where people go for financial services. Hence Microsoft’s 1996 attempt to buy Intuit, the manufacturer of Quicken and market leader in this area.

Although such programmes are not yet very popular in Europe, the experience of US banks should be watched closely. If personal finance packages gain more general acceptance in Europe, banks would need to be prepared because they could become mere suppliers of a commodity product without an end-customer base. Such packages might also encourage UK residents to bank with non-UK institutions, though they could equally well draw foreign banking business into the UK.

6. How easy is it to navigate the Internet?
A significant problem for Net development is access. Even the best financial products and services advertised on the Internet will attract few buyers if the consumer cannot find the information quickly and cheaply.

As already indicated, a rapidly-growing number of financial services providers already maintain Web sites which are well worth a visit. Some offer on-line applications for information or subscription services for certain types of investment. Others are information-only but tell the investor how to obtain further material. With the aid of a web browser (for example Netscape’s Navigator or Microsoft’s Internet Explorer), all of these sites ought to be easily reachable by any potential customer. A variety of on-line search engines can also assist, including AltaVista, Lycos, and Yahoo. That, at least, is the theory.

Putting this theory to the test does not, however, always produce useful results. One member of the group carried out several searches using AltaVista at various stages between June 1996 and March 1997 to see what results might be achieved from crude searches for information of the sort that a prospective investor might think to make for himself. The equipment used included a 60 MHz Pentium PC running Windows 3.1 (still fairly typical for the home PC market) and a 28,800 baud modem. Searches were carried out during the afternoon and early evening (London time) on several weekdays, which is one

---

1. Microsoft’s Internet Explorer is available free at the Microsoft Internet site: http://www.microsoft.com. Certain versions of Netscape’s Navigator are also available free, and can be found at http://www.netscape.com
Second generation sites: New personal finance sites are being set up all the time. Here is a
digest of some (free and subscription-based) as cited by the Financial Times in January 1997:

- Trust on the Internet (http://trustnet.co.uk) has free information on UK-registered investment
  trusts and other offshore investment companies, along with daily indices and world exchange
  rate details.
- Stock Data Corporation (http://stockdata.internet/stockdata) provides price and volume
  information for stocks and indices tracked on three US exchanges.
- Richard Majena's SMART Stock Market Timing Letter (http://members.aol.com/smartlet/
  home.html) has a market update and market track information.
- The Swiss Investment Marketplace (http://www.jmi.ch/jmi) has some good information for
  private investors (even if its aim is to make you feel guilty for not hedging your portfolio in Swiss
  francs).
- Fundscape (http://fundscape.com) is a commercial service offering investors the chance to
  track the performance of mutual funds.
- Foreign exchange consultant Atrra management Services has set up Inside the Market (http://
  www.textor.com/markets/attrax) - a daily forex newsletter. This is part of the "Square Mile" site
  which offers good business intelligence.
- The Association of Investment Trust Companies (http://www.ilt.co.uk/aitc) is one of the new
  sites available through Interactive Investor - along with Global Asset Management, Micropal
  and various FI magazines. The AITC site has a directory and profiles of UK investment trusts.
- Findex (http://www.findex.com), put up by St. Clair Financial Index, is a searchable database
  of financial media and institutions which is a useful, easy-to-use site once one gets past the
  "lobby". It includes many of Citibank's country investment guides.
- The "Market Movers" investment analysis is available through Pinson Associates Financial
  Centre (http://ffco.com) site, a useful and interesting review of activity on Wall Street. It is also
  easy to use with regularly updated quotes and charts.
- Investec (http://www.investec.com/index.html) boasts interesting electronic stock and
  commodity trading information, including The Cutting Edge - with an introduction to chaos
  theory: "a new paradigm in trading".
- Bankers Trust Global Research (http://www.bankerstrust.com/global/global.html) has details
  of the firm’s daily US and European financial newsletter. A very good, user friendly site with solid
  analysis and a good calendar of upcoming events.
- Canadian Stock Market Reports (http://canstock.com) is an information source covering the
  four Canadian exchanges. Free trial subscriptions are available for evaluation purposes.
- MSN Global Inc (http://www.msnglobal.com) provides research on global investment
  opportunities. It is a nice straightforward site.
- Global Asset Management (http://www.ukinfo.gam.com) has put up a site with a good deal
  of helpful information and details of the e-mail based GAMClub.
- Numa Financial Systems’ NumaWeb (http://www.numa.com) provides comprehensive
  resource information for the derivatives market. Lots of clear, logical links make it easy to
  navigate and the " neural broker" feature is especially innovative.
- Moneyweb (http://moneyweb.co.uk) is probably the most comprehensive UK personal finance
  site. The "Hotpapers" link takes one to an extensive library of essays and institutions’ homes
  pages.
- Investorama (http://investorama.com) is a very comprehensive US personal finance site,
  including links to other financial sites.
- Interactive Investor (http://www.ii.co.uk) is an almost equally comprehensive UK site - with
  a particularly useful contact list of IFAs.
of the busiest periods of the day, since it represents early afternoon on the East Coast and early morning on the West Coast of the US.

A search in June 1996 against the phrase "Life Assurance" proved rather disappointing. AltaVista reported 3,000 relevant or possibly relevant pages. Of the first ten, four were errors (i.e. references to pages which no longer existed), three offered information on mutual funds marketed by a Canadian life assurance company's fund management arm, one was an advertisement for the salesforce of a company marketing non-life products, one offered medical insurance services to inhabitants of three US states, and one site refused to load at all. Searching all of these pages (including, in some cases, associated pages) took nearly 40 minutes and turned up nothing of value.

The same search one afternoon in September 1996 was a little more productive: only two errors this time, two sites with Standard & Poor's credit rating data of life insurance companies, three sites with image-only advertisements for different overseas companies selling life products in their localities, and one site with a news feature on the retirement of the CEO of a South African life assurance company. However, the remaining two sites referred to the services of firms of UK intermediaries offering life assurance and similar products. Examining all ten sites and associated pages took 24 minutes.

Repeating the search in March 1997 provided a similar mixed bag of results. Three of the top ten were S&P ratings once again. Two offered the services of overseas life assurance companies (and a third would also have done so, judging by its name, had it not been an error). One referred to an article to do with electronic engineering (where the phrase "life assurance" had been used metaphorically in the title of the article). One offered non-investment life products to New Zealanders. However, one was an image-only advertisement (with telephone number to call for further information) posted by a UK life assurance provider, and a tenth was a comprehensive site posted by Sun Alliance, with a lot of information about products on offer and how to obtain further information. As a human touch, a section of the site was devoted to an attractively presented trivia quiz.

Searches in September 1996 and March 1997 against "PEP" and "personal equity plan" yielded mixed results. In the UK, "PEP" is almost a household word, but it is a not uncommon acronym in fields other than the investment marketplace, and searches against "PEP" produced largely irrelevant results accordingly. The September search against "PEP" indicated 10,000 possibly relevant hits. The searcher had to descend to hit 40 before finding a hit (Fidelity) which described how the investor might find out more about and, in time, buy a particular personal equity plan. Of the first ten hits, six were connected with an environmental project on the West Coast of the US, one was for a company offering skills training courses and the other three were erotic offerings of one sort or another. Repeating the search in March 1997 improved the quality slightly with two hits in the first ten directing the investor to Scottish Amicable's PEP range. The other eight were irrelevant for various reasons.
Searching against “personal equity plan” improved the results in each case. Even so, the September 1996 search yielded only one relevant hit in the top ten (Fidelity, again); the remainder were either statistical or generic information on PEPs (one of which would not load at all). The same search in March 1997 was much more successful, however. All of the top ten were potentially relevant, judging from their names and brief descriptions in the *AltaVista* search report. The top four, though not pages offering PEPs for sale, were useful analyses of the PEP product in its different forms provided by a service called AAA Investment Guide. (By way of a minor criticism, however, it was not very clear from the pages themselves, once retrieved, that they were a part of a larger Web site that had information on different types of investment products.) Hit five was placed by an Ipswich firm of solicitors who carry out a variety of investment management services as well, and hits six to ten all related to pages in the Norwich Union Web site, informing prospective investors of NU products and providing generic advice on PEPs and when/how to buy them.

Lastly, the searcher searched against “pension”. September 1996’s results were of little use – nothing useful in the first ten of 50,000 matches. March 1997’s search was in fact no better, producing ten different but equally useless top results.

This analysis is simple – perhaps even simplistic – and far from exhaustive. But it does disclose two fundamental problems:

- First, unless the consumer knows in advance which Web pages he is going to retrieve, he has to devote time and money to searching on the Net for information he believes that he needs. It is still without doubt true that surfing the Net for general information is likely to consume more time and resources and to yield less satisfactory results than spending the same or less time on a periodic basis with a financial adviser or, perhaps, scanning the financial press for inspiration.

Better tools and training will help the searcher to refine his results to a degree. In fact, *AltaVista* has acknowledged that it can be distressing to be told that there are 50,000 entries to one’s search and has now introduced a feature called “Live Topics”, where the searcher can refine a search by specifically including or excluding words shown in checklists that are considered by the designers of *AltaVista* to be relevant to the original purpose of the search. Thus, with “PEP”, “Live Topics” offered various terms to include or exclude, such as “share”, “trust”, etc. Selections are made using check-marks in YES and NO boxes, rather than requiring the searcher to enter the terms from the keyboard himself. Still, though, Internet searches for investment products and advice are laborious.

- Secondly, there is still much that is wrong or inconsistent with Web page design. If a page is very long, or loaded with unnecessary images and graphics, the searcher may lose patience waiting for it to load in full. Some are misleadingly titled or composed without regard to the manner in which
a search engine like *AltaVista* picks them up. *AltaVista* is essentially an engine which matches the searcher's request verbatim with what it finds on the Net. This means that a page called "Nothing to do with life assurance" will rank as highly as one called "All you need to know about life assurance".

The world of search engines: As a December 1996 FT article pointed out, search engines "are sites you dial up with your browser that help you search through the other offerings of the Web... Without these tools, the Web would lose much of its usefulness, since it is too large and complex for browsing or surfing."

There are lots of search engines available. To start with are the general search engines, which search out information on any topic:

- **AltaVista** (http://altavista.digital.com) has the largest Web index: 31m pages on 476,000 servers and over four million articles from 14,000 Usenet groups. It recently added a multi-lingual capability (14 European languages), as well as sub-categories focusing on particular issues. One of these is finance. Although easy to use in basic mode, it also allows for advanced Boolean searches.

- **Lycos** (http://www.lycos.com) is also very user-friendly. Its numerous sub-categories and "search areas" (like City guide, Stock finder, etc.) make it particularly helpful for information relating to the financial industry. It also provides commentary and suggestions, top news headlines and a companies index.

- **Yahoo** (http://www.yahoo.com) is also a general search engine, which categorises data in 14 main interest areas. It provides daily news and stock quotes, and has basic and advanced search options.

- **Excite** (http://www.excite.com) is another comprehensive search engine, featuring an index of more than 50 million Web pages. It links to Search Voyager (http://voyeur.mckinley.com/voyeur.cgi), which allows a peek over another user's shoulder. It also has statistics on the most popular categories.

- **Infoseek** (http://info.infoseek.com) offers a one-stop-shop covering everything from software to searches for specific e-mail addresses.

- **Webcrawler** (http://webcrawler.com) is a very simple but very powerful search engine. It maintains a searchable index which is regularly updated.

- **All4One** (http://www.all4one.com) is the search engine of search engines. Rather than limiting itself to a single database, this service runs a search through several (AltaVista, Lycos, Yahoo and Webcrawler) and provides the results in separate frames (which means that one must have a "Frames" enabled browser).

If one is looking for articles, newsgroups or text-based information, **DejaNews** (http://www. dejanews.com) provides an excellent service. It searches through Internet newsgroups, classifieds, various publications and academic articles for key words. If one is looking for shareware, several search engines exist, including:

- **Tucows** (in the UK, http://www.tucows.co.uk/tucows) which searches out shareware available on the Web.

- **Shareware.com** (http://www.shareware.com) which is similar to Tucows but also pinpoints the location nearest the user where the shareware is located; in this way, download time is minimised.

There are also "people locators", which assist in finding a specific individual or e-mail address:

- **WhoWhere** (http://www.informi.co.za/search/who_where.htm) is a particularly good tool.

- **Bigfoot** (http://www.bigfoot.com) is similar, with the added ability to get lifetime e-mail addresses.

There are also numerous specialised search engines. For example, **The Global On-line Directory** (http://www.god.co.uk) focuses on UK-based Web offerings. Similarly the **Swiss Search Engine** (http://www.search.ch) focuses on
Switzerland. There are now so many different search engines that a link page exists (http://www.pitmen.net/~rickyl/index.html). This is admirably maintained by a private individual, Rick Johnson, and provides extensive listings and descriptions of search engine types. More advanced search engines, usually in the form of "intelligent agents", are also available. These generally come as pieces of software. They fill words and ideas into context and learn from their mistakes. AutoBender (available at http://www.agentware.com) is a good example.

Increasingly, users can make use of a number of sites specialising in a particular subject. Several cater to the financial services market, and to personal finance in particular. These sites often provide "link pages" – Web pages which have hundreds, sometimes thousands, of links to other pages within a given field.

Once one finds a site that is of interest, one is faced with the problem of having to return to gather new information. This is made easier by Freeloader (http://www.freeloader.com) – a software program which downloads pages on a periodic basis. This can be programmed to be done when the user is not there, thereby avoiding the need to wait.

Another piece of useful software is CyberPilot Pro by NetCarta. Although not free (it costs $65, information available at http://www.netcarta.com), this goes on-line and maps Web sites, returning location details for information which may fill the search criteria. It does this by use of "spiders" – agents which surf the Net for you. Unfortunately, "spiders" do not have a good reputation on the Net. Not only do they significantly increase capacity problems but many pages are finding ways to lock "spiders" out, fearing that a badly programmed "spider" may actually damage a Web site.

Search engines are becoming more complex. Already several companies are working on new types of filters, some using advanced neural networks. US-based Beatty Network uses collaborative filtering, first developed at MIT. These agents are so advanced that they can actually make suggestions to the user based on the preferences of other agents owned by people with similar interests. Some companies – like IBM through its World Avenue "cybermall" – will actively collate user information as the user interacts with any of the retailers. The agent will "learn" the types of products that the user is interested in and alter displays accordingly.

Increasingly, large companies are becoming interested in these kind of search engines. For example, Andersen Consulting has already developed BargainFinder, a search engine which scans the Net for the lowest price on a particular product. It has now taken this one step further and developed LifestyleFinder, which – once programmed with an individual’s preferences – searches the Net on a continuous basis to find items which may be of interest.

Search engines differ in the way they work, of course, as does the level of complexity possible in a search. For example, it is possible to create quite complex searches – using Boolean logic routines and subsets – in advanced versions of many search engines. But to do this a user would not only have to be familiar with the logic of search methods (not as common as some assume) but would also have to feel sufficiently comfortable with the technology to attempt using advanced versions of it, which is unlikely to be the case for most people in the near future.

Consequently, those designing Web sites devoted to financial products should not assume that potential users possess anything but the most basic abilities. It is also wrong to assume that people make use of only the most sophisticated Internet browsing software with the fastest modems. If a site is designed for viewing with the latest versions of browser software, many users will be put
off rather than impressed since they will receive most of the new functions or graphics as errors.

In the end, the best way of finding the right Web sites quickly will be the development of specialist search engines devoted to personal financial products, or greater use of the specialised electronic financial services sites that are starting to become available. As the marketplace in personal products continues to internationalise, this is likely to become a major opportunity for software and/or financial service suppliers, though they will need to examine conditions in a variety of legal jurisdictions. This is clearly a costly proposition, and interest in Internet-supplied financial services from within the UK may be insufficient to make it viable. (For the present, a search engine that covers the United Kingdom is sufficient for most UK users.) It might also be a project that would have to be led by an independent organisation, given the highly competitive nature of the financial marketplace.

A further approach lies in Web sites which act as "link pages", such as Interactive Investor, MoneyWorld and Investorama. This can be a very cost-effective solution, though with three problems:

- the difficulty some users seem to have in locating such services in the first place;
- the continuous updating which such pages require if they are to remain current; and
- the fact that the services on such pages, while free for users, are not always free for "exhibitors".

The pages are therefore likely to be incomplete because some providers will not be there. Where such pages are maintained as a public service — as in the case of the French site Qualisteam (http://www.qualisteam.com/aconfeur.html) — they tend to be non-judgemental and do not attempt to classify their lists (except perhaps geographically).

Fortunately, or unfortunately, the big Net companies are not standing still. Microsoft and Netscape, for instance, are both working on what is called "dynamic HTML" technology, which will turn static Web sites into full-fledged programmes with embedded intelligence. These will run on the user’s computer, rather as Java and Active-X do. No doubt, in the end, this will be a big leap forward; in the short run, it will likely make browser’s task even trickier.

7. The effect on UK IFAs (and what they can do about it)

The ability of the Internet to put consumers of financial services in direct touch with providers poses a threat to the middleman, notably in the market for "commodity" products where price, rather than advice, is the main determinant.

Using the resources of the Internet to acquire financial skills and carry out his own research, the consumer is increasingly in a position to identify his needs himself, and then instruct an intelligent agent to find the best product to match
them. Many publications – including the Financial Times (http://www.ft.com) – already offer more comprehensive services on their (free) Web sites than they do in their (not free) printed publications. A number of leading financial institutions also put free research material on their Web sites. It is only a matter of time before link pages and specialised search engines successfully automate the collection of such information; indeed, it is already starting to happen.

Where, in such a world, is there a place for the hard-pressed independent financial adviser (IFA)?

IFAs on the Web: Although few UK IFAs have Web pages, the Net is a useful source of information about them. Interactive Investor (www.ii.co.uk) and MoneyWorld (www.moneyworld.co.uk) carry lists of UK IFAs. Some investment companies also include “IFA locators” on their Web sites, eg:
- Norwich Union at www.norwich-union.co.uk/ftadvice/cifa.htm
- Scottish Provident at www.scotprov.co.uk/index/oinfo.html
- Scottish Amicable at www.scottishamicable.com/sicotam/3-7page.html

One site – www.amp.com.au/1-4e.htm - provides a list of questions to ask an IFA on first contact. Another – www.mfs.com/education/work_calc/invasive.html - helps the investor identify the key points he needs to put to his adviser. A comprehensive source of personal finance advice - a series of reviews and publications - is published by Dalbar at www.dalbar.com/pfo9600.htm.

MoneyWorld Guides offers an overview of how to select an IFA (www.moneyworld.co.uk/moneyworld/faqs/finfaq3.htm) as well as an extensive list of IFAs at www.moneyworld.co.uk/ukpfd/out-aff.htm. In this respect, UK web sites are more advanced than their US counterparts.

Several IFA referral pages are also available on the Web:
- the International Association for Financial Planning (IAFP) offers a financial adviser referral service at www.iapf.org/e1.html, where IFAs can list services at no charge.
- “Find an IFA” at www.seven.net/moneyweb/search/search.html
- The IFA Association at www.ifao.org.uk.

There is even a service specialising in “environmentally friendly” financial advice offered by Gaia at www.u-net.com/~gaia/home.htm.

The IFAs’ dilemma is made worse by the fact that few of them yet possess computers or seem inclined to find out about new technology, both because of the cost and the conservative nature of their business. Clearly, many investors will continue to need financial advice and will remain loyal to their advisers. But IFAs will have to develop their computing expertise and adapt their role to the Internet age if they are to avoid being pushed into a backwater.

The growth of IFA networks could open up the way to closer Internet involvement for them; but at the moment most firms who are in a position to join such networks (and that is still a minority) communicate with each other via their own computer links or through physical exchange of computer disks. However, specialised services and software for IFAs are becoming available. One IFA tool is Interactive Investor. Others (eg. TRDL’s Aequos) are still
non-Net but have the potential for rapid growth via the Internet. Another initiative is Origo’s Exchange, a joint venture between a group of insurance companies and AT&T, as technology supplier, to provide quotations for insurance products. At the moment this is a proprietary on-line service, but the intention is to make it available over the Web with a transaction capability and links to other insurance-related and IFA Web sites.

8. The way ahead – how to make the system easier for the investor

If the Internet is to become a major market for personal financial services, it will have to convince the consumer that it is better or cheaper than other distribution mechanisms. As indicated, a small number of wealthy individuals already use it to conduct their financial affairs, though they are unlikely ever to be sufficiently numerous to sustain a large market. More significantly, the Internet has the potential to become a mass marketing tool, and it is here that the vast majority of providers will initially aim their services.

The qualities the Internet will need to demonstrate are value, service, convenience and security. If financial providers cannot make Internet service financially attractive, there will be no incentive for consumers to switch. Similarly, they must offer a level of service such that consumers see an advantage in dealing over the Internet rather than through the traditional middle man. Providers are getting better at this, as the rapid development of telephone banking and insurance demonstrates. But back-office arrangements still have some way to go before they can cope with the real-time requirements of a large Internet-based business. If the Net is to develop mass appeal, the consumer will also have to be able to find his way around it with greater ease.

One of the Internet’s strengths is its ability to pull together services from a number of suppliers and package them in an attractive way to form a single platform. An example of this might be the sale of foreign retirement homes to UK investors through a comprehensive package which includes legal work, surveys, local taxes, financing arrangements, and even advanced add-ons like currency hedges. Medical insurance might be a further feature.

Users will also need to have sufficient confidence in the Internet to entrust it with their financial affairs, which is not currently the case because of the perceived security risk.

How might consumers be encouraged to have greater confidence in the Internet?

One suggestion put forward by the working group is that UK regulators should issue a “kitemark” to financial Web sites which meet certain criteria. The mark would indicate, for example, that the provider was officially regulated (by IMRO, the PIA or another regulator), that the statutory protections applied and that certain security conditions were met. But it would go beyond this, in that it would provide some assurance that regulators monitored the site and the claims it carried.
The Internet and Financial Services

So far, UK regulators do not see a role in providing this type of authentication. They feel it is beyond their remit and might expose them to legal hazard if the sites were tampered with. Of course, this authentication role is always open to trade bodies or other entities that have an interest in establishing “safe areas” for investors. A link page might, for example, be created on which only “approved” companies were listed as hyper-links.

9. Conclusion

The personal financial services market on the Internet is, at present, very limited; but in our view it has the potential to achieve mass market status. The Internet’s convenience, its ability to marshal large amounts of information, to search out attractive investments, and handle the resulting transactions make a formidable combination. But to achieve this, considerable work needs to be done to make the medium more user friendly, to ensure that economic benefits are passed on to the consumer and to build trust in the system. The question at the moment is who will provide this push, and how quickly.

Established financial service institutions are playing a watch-and-wait game. Understandably, they are unwilling to make a large financial commitment to an untested medium. On the other hand, they know that the Internet’s novelty could provide an opening for a wholly new set of competitors, unburdened by the costs of the past. So they need to be on their toes. The IFAs are also holding back, though possibly out of ignorance rather than caution.

We expect that a combination of technological breakthrough and the emergence of bold innovators will deliver the impetus over the next two or three years, leading to a surge in financial activity over the Internet. At that point, the personal finance industry, which is already having to cope with the challenge of telephone marketing, will face further deep structural changes: the consumer will be in a much stronger position to decide where and how he does business. Our sense is that he will increasingly deal directly with the service provider, using price as his main guide. However one should not underestimate the value that people attach to sound advice and personal attention. For this reason, there will continue to be a role for the intermediary, though perhaps in a very different form.
SECTION TWO: KEY FINANCIAL SECTORS

Chapter three: Insurance and reinsurance

Summary: Insurance is an area where Internet take-up has been late, but where the potential is huge (though the industry is also hedging its bets with ambitious proprietary systems as well). There are already dozens of UK insurance sites, some offering on-line quotes – even for non-standard risks. Lloyd's has also launched a service offering Net access to all underwriters and managing agencies via a common gateway, and reinsurers are at least using the Web as a source of information. Among the brokers, more than one has launched a special Internet-based insurance service. Despite this, the industry underestimates the potential of the Net – both positive and negative (in particular, the threat of disintermediating retail brokers and boosting remote markets, e.g. Bermuda, at the expense of conventional centres).

Chairman: Rowan Douglas  WIRE
Vice-chairman: Gilles Bonvarlet  Brockbank Underwriting
Rapporteur: Rowan Douglas

Working group members:
- Antony Aitken: Transition Partnerships
- Michael Higgins: WREN Group Services
- John Johnstone: UAP Provincial Insurance
- William Kinsley: Alexander Howden Group
- Tim Leslie: SHL Systems

The group included other members who have requested that their names not be used.
1. Introduction
The UK general insurance market and the world commercial and reinsurance markets (of which London is the leading centre) have remained relatively immune to the advance of sophisticated electronic networks, although there is some use of proprietary software systems and local area networks.

The retail segment of the general insurance market is still largely intermediated by brokers; direct telephone distribution marks the greatest extent of technological progress (at least in the UK). Since it is extremely fragmented, this structure has stymied the development of large-scale proprietary electronic networks.

In the reinsurance markets, the complexity and longevity of contracts have hindered the introduction of standardised forms, and this has reduced the opportunity for electronic transmission of risk information. Furthermore, the subscription nature of the reinsurance market (which brings companies and syndicates from all over the world on to a single contract, or slip) makes it difficult to introduce common systems. Paper still reigns supreme at the international level, though this, as we shall see, is beginning to change.

The significance of the Internet is that it has the ability to circumvent many of these obstacles to technological co-operation. It offers common platforms and protocols through which companies in both local and global markets can communicate without the need for complex agreements. Indeed, there are signs that this is now happening; for once, insurance and reinsurance could be at the forefront of a new business communications medium.

2. Basic assumptions
The working group was fortunate to have a variety of viewpoints represented among its members, but all were agreed on the key characteristics of the Internet as it relates to insurance:

- It is global and ubiquitous. Most individuals and organisations already have the potential to connect to the Internet. This is significant for both domestic general insurers and global reinsurers.
- The Internet communications protocol is generic, cheap and simple.

However, the group also agreed that the Net suffers from several handicaps:

- perceived inadequacies in security;
- slow speed and low capacity; and
- a measure of social resistance to take-up.

1 World commercial insurance is the provision of insurance to commercial organisations, which often requires the collaboration of the international insurance market. Reinsurance is the protection of insurance companies against large scale and catastrophic loss. Insurance companies routinely purchase reinsurance policies to offset extreme events and exposures.
The Internet and Financial Services

In spite of this, the opportunity that the Internet provides to obtain, process and distribute information about risk suggests that it has genuine potential to reshape the insurance industry. It was also felt that these handicaps were likely to be temporary. The market will find solutions.

3. Current state of Internet usage

The group surveyed a number of user categories (UK general insurers, Lloyd’s managing agencies, etc.) to gain information about current usage of, attitudes towards and plans for the Net. The results were plotted on a table which lists the issues on one axis and type of user on the other.

Use of the Internet

<table>
<thead>
<tr>
<th>Regular user</th>
<th>Information/research</th>
<th>Communication</th>
<th>Value-added Services</th>
<th>Product Sales</th>
<th>Regulatory Implications</th>
<th>Interface/IT/systems</th>
<th>Alternatives</th>
<th>Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsing</td>
<td>Concerns over security</td>
<td>Keen</td>
<td>Experiencing</td>
<td>Prepared</td>
<td>Prevents</td>
<td>Studies closed</td>
<td>Use to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>risk - but</td>
<td>viruses</td>
<td>systems</td>
<td>limit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>nervous</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occasional</td>
<td>Aware</td>
<td>Learning</td>
<td>Experiencing</td>
<td>Watching</td>
<td>No scandals</td>
<td>Stand-alone PCs</td>
<td>Could be</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>marketing</td>
<td>opportunity</td>
</tr>
<tr>
<td>Not yet</td>
<td>Waiting</td>
<td>Not aware</td>
<td>Not aware</td>
<td>Not aware</td>
<td>Waiting</td>
<td>Waiting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Never</td>
<td>Relies on broker</td>
<td>Relies on fax and the phone</td>
<td>Not aware/ &quot;not safe&quot;</td>
<td>Not aware</td>
<td>Messy</td>
<td>Not aware</td>
<td>Long way to</td>
<td></td>
</tr>
</tbody>
</table>

Despite a number of initiatives, insurers and reinsurers have had difficulty coming up with a generally accepted business model for the Internet. But the industry is now advancing beyond the level of home pages – which provide little more than marketing information – to higher levels of sophistication as it begins to use the Internet as a business tool.

Perceptions of the Internet: Broadly speaking, the more exposure a person has to the Internet, the more likely he is to see its potential. However, people at a senior level in insurance companies tend to have the least experience of the Internet. Conversely, the members of IT departments who do understand the Internet are often those who are least able to articulate its business possibilities. Moreover, some IT departments, fearful of the impact on their existing systems, have tended to under-emphasise its potential.

The problem is communication. Few insurance companies have people who understand the Internet and what it can do. Fewer still have people with this understanding in the boardroom. However, this situation is beginning to change. As the quality of insurance-related information on the Internet improves and more companies develop ways to take advantage of it, a more positive attitude is developing. As a result, senior management is increasingly placing the Internet on its agenda.

Deployment among UK general insurers: Before examining Internet usage, it is worth reviewing the broader state of play.
Electronic trading has established itself on a modest scale among insurance brokers and is increasing as a consequence of electronic data interchange (which offers the benefits of lower costs and more accurate and timely data). This EDI traffic is generally not available on the Net. Rather, it uses proprietary software systems (e.g. Mysis, Continuum Re, PolicyMaster, ITT Quotet, etc.), and travels on value-added network services (VANS) such as IBM’s Information Exchange and GEIS’s Tradenet.

To meet the competitive threat from direct insurance writers like Direct Line, a personal lines initiative (Polaris) was set up to provide insurers and software houses with a standard framework for the development of insurance products. The aim is to reduce the time taken in bringing products and/or rating changes to market from the current 3-6 months to, potentially, overnight. Similarly, a Commercial Lines Market Initiative (CLMI) has been established to develop parallel electronic trading standards for commercial lines business.

**CLMI and Polaris**

**Commercial Lines Marketing Initiative (CLMI):** CLMI was formed by 13 insurers and nine national brokers to develop standards for transacting commercial insurance business by EDI so as to improve service and reduce costs. They have adopted existing EDIFACT messages for home and motor insurance to accommodate packages as well as commercial motor business. More recently, as complex classes of business have been examined, different message formats have been merged into a common one, which will be used in conjunction with other forms of electronic trading.

ITT Quotet recently developed a quotation facility (Gilt Edge) which incorporates CLMI standards and provides POS quotations for small commercial package businesses. This will be capable of transacting business with insurers’ systems using EDI. Other software houses have indicated that they will adopt CLMI standards.

**Polaris:** Polaris was formed by seven insurers in 1994 to counter the threat from direct insurers by introducing standards for electronic trading. These enable insurers to issue products and product changes in a much shorter timeframe than before.

A PC-based software tool called ProductWriter has also been developed by Polaris to provide insurers with the ability to define their products — not just underwriting and rates, but also contents of printed forms and format of electronic trading messages. These can then be put in a consistent format for transmission to participating software systems for onward distribution to the intermediaries. This method of standardisation — using a data dictionary — allows software houses to incorporate new insurance products, amendments and rate changes very quickly and at low cost. Initially, it only supported motor insurance, but it has now been expanded to include home insurance products, and the CLMI data dictionary is being incorporated into ProductWriter so that the software can be used for the design and maintenance of other products.

Currently, personal line EDI transactions follow Brokernet (UNGTDI) standards, but will probably embrace the more widely-adopted EDIFACT standards within the next two years. Commercial line EDI transactions already conform to EDIFACT standards.
The Internet and Financial Services

According to a 1996 survey by the British Insurance & Investment Brokers Association, 1 40 per cent of all new motor business written by participating intermediaries is now transacted using EDI. This is expected to rise substantially and to expand to other transaction types (mid-term adjustments, renewals, etc.) by the end of the decade. The BIIBA survey also showed that 55 per cent of the overall personal lines market (which includes home business) is controlled by intermediaries, 25 per cent by direct writers and 20 per cent by others. Since then, direct writers have moved aggressively into the home market, and have also increased their share of private motor business.

In the commercial lines market, most business is still transacted through intermediaries, with only one major insurer having established a direct (i.e. telephone) sales operation.

In spite of these initiatives, however, the impact of proprietary networks has remained small, partly because of the cost and partly because of the administrative difficulty of obtaining agreement on common standards. It is desirable, therefore, that these networks be converted to allow Internet compatibility; this would immediately simplify communication and link them to a much larger potential market.

Internet developments: The reason is that common standards have already been defined for the World Wide Web – and this has opened up a previously unexploited marketing channel, with profound implications for the insurance sector. Since the Web became commercially available, however, not very many UK-based insurance companies or intermediaries have yet created their own Web sites. The box below gives some of the major retail orientated sites available in the UK as of late 1996.²

<table>
<thead>
<tr>
<th>Company</th>
<th>Address</th>
<th>Product type</th>
<th>On-line quota request</th>
<th>On-line quota given</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admiral Insurance</td>
<td><a href="http://www.admiralins.com">www.admiralins.com</a></td>
<td>Motor</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Automobile Association</td>
<td><a href="http://www.theao.co.uk">www.theao.co.uk</a></td>
<td>Motor</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Personal accident</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Property</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pet &amp; horse</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yacht &amp; boat</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Travel</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>AXA</td>
<td>axa.co.uk</td>
<td>Motor mechanical</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Canopy motor policy</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Severn motor policy</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Venture liability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Barclays</td>
<td><a href="http://www.barclays.co.uk">www.barclays.co.uk</a></td>
<td>Travel</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Chatham Insurance</td>
<td><a href="http://www.chathaminsurance">www.chathaminsurance</a></td>
<td>Home building &amp; contents</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Brokers</td>
<td></td>
<td>Travel &amp; holiday</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Private medical</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Working from home (UPA1 punity policy)</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Churchill</td>
<td><a href="http://www.churchill.co.uk">www.churchill.co.uk</a></td>
<td>Motor</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Household</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


2. This list was provided by WIRE Ltd.
<table>
<thead>
<tr>
<th>Company</th>
<th>Address</th>
<th>Product type</th>
<th>On-line quote request</th>
<th>On-line quote given</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial Union</td>
<td><a href="http://www.commercial-union.co.uk">www.commercial-union.co.uk</a></td>
<td>Home contents</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Cornhill</td>
<td><a href="http://www.cornhill.co.uk">www.cornhill.co.uk</a></td>
<td>Motor</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wedding</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Travel</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Health</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Life</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mortgage</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Direct Line</td>
<td><a href="http://www.directline.co.uk">www.directline.co.uk</a></td>
<td>Motor</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>General Accident</td>
<td><a href="http://www.ga.co.uk">www.ga.co.uk</a></td>
<td>Motor</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home building &amp; contents</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Travel</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Guardian Insurance</td>
<td><a href="http://www.gre.co.uk">www.gre.co.uk</a></td>
<td>Motor</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home &amp; contents</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assets health</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PC</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home greens private pilot</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zephyr yachts &amp; motor boats</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Professional indemnity:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Professional</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Other</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High value household &amp; fine art</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voyager cargo</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Insurance Club</td>
<td><a href="http://www.insuranceclub.co.uk">www.insuranceclub.co.uk</a></td>
<td>Household</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>(Independent Insurers)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterSure (Torchl)</td>
<td><a href="http://www.interSure.co.uk">www.interSure.co.uk</a></td>
<td>Motor</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Household</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Wedding</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Travel</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pets</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Lincoln National</td>
<td><a href="http://www.moneymworld.com/lincoln">www.moneymworld.com/lincoln</a></td>
<td>Health</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Norwich Union</td>
<td><a href="http://www.norwich-union.co.uk">www.norwich-union.co.uk</a></td>
<td>Motor</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Household</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Household</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Travel</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Preferred Direct</td>
<td><a href="http://www.pdinsure.co.uk">www.pdinsure.co.uk</a></td>
<td>Motor</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home building &amp; contents</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Prospero Direct</td>
<td><a href="http://www.prospero.co.uk">www.prospero.co.uk</a></td>
<td>Motor</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RBS Insurance</td>
<td><a href="http://www.colinbeck.co.uk/rtbc">www.colinbeck.co.uk/rtbc</a></td>
<td>Commercial &amp; business</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Consultants</td>
<td></td>
<td>Travel</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Leisure &amp; Guard clubs &amp; societies</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Royal Insurance</td>
<td><a href="http://www.royal-group.co.uk">www.royal-group.co.uk</a></td>
<td>Motor</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Sun Alliance</td>
<td><a href="http://www.worldsilver.nl/index.html">www.worldsilver.nl/index.html</a></td>
<td>Motor</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medical</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Travel</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accident</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>UAP Provincial</td>
<td><a href="http://www.uap-provincial.com">www.uap-provincial.com</a></td>
<td>Motor</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Home</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Private health</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Commercial</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Worldcover Travel</td>
<td><a href="http://www.worldcover.co.uk">www.worldcover.co.uk</a></td>
<td>Travel</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

This sounds more impressive than it is. In fact, the majority of these sites are information-only, with limited feedback possibilities. They provide telephone numbers (and, in more innovative cases, an e-mail link) to gather personal and risk-related information. Quotations are available on-line in a few instances,
The Internet and Financial Services

but mainly for standardised insurance products such as travel and motor business.

That said, one or two underwriters have developed Internet-based automated underwriting services for more complicated classes of business. Worldcover Direct Limited (http://www.worldcover.co.uk), a Cardiff-based travel policy writer, has also developed an automated quotation service which allows clients to purchase policies on-line by credit card. Policyholders can also make claims on-line and receive emergency assistance. In 1995, for instance, Hiscox Underwriting introduced automated quotations for professional indemnity insurance and followed it up in 1996 with a similar service for general aviation. Guardian Royal Exchange has a small Internet business insuring PCs.

Key issues for general insurers: In considering the Internet, the general insurance industry has to bear several things in mind:

- The Internet could provide general insurers with a new means of reaching consumers and brokers, but it could also wipe out their existing distribution channels.
- Concerns persist about Internet capacity, reliability, speed and security. Although these may be declining, greater confidence and market penetration will have to be achieved before an industry-wide commitment to electronic trading over the Internet is likely to occur.
- More significantly perhaps, a considerable number of small to medium-sized brokers have already invested in proprietary systems to conduct business with insurers using EDI. Since these systems also provide them with back office support, it is unlikely that they will consider switching to the Internet unless driven by customer demand or substantial cost savings.

Deployment by Lloyd's agencies: Managing agencies oversee the operation of syndicates, the units that underwrite business at Lloyd's. They vary in size from the very large (like Wellington Underwriting Agencies with £750m in premium income) to smaller agencies with income of £20m-£50m. Some agencies currently have Web sites (such as Hiscox and Brockbank) and many more use the Internet to access information. Only a few, mostly smaller, agencies are not connected to the Internet at all.

The working group surveyed IT directors in twenty managing agencies and asked questions in six key areas. The conclusions can be summarised as follows:

- **Internet connectivity:** Most respondents had a standalone dial-up connection and very few were networked. The departments likely to be connected are generally IT or systems, followed by underwriting of marine, motor, non-marine and personal lines. Other departments found to be connected included reinsurance treaty, agency management and finance.

---

1. The group realised that aiming its enquiries at IT departments skewed responses. However, it was felt that IT departments — necessarily at the core of any company’s Internet strategy — would provide a good insight into Internet-related activity.
Insurance and reinsurance

- **Internet usage and functions (by frequency):** Main uses of the Net were:
  - communication via e-mail;
  - technical support (downloading software releases, help lines, etc.);
  - risk research;
  - general information (weather, etc.);
  - insurance and reinsurance market news; and
  - research into assureds' backgrounds.

- **Internet presence (Web sites):** Few agencies had their own Web sites as of June 1996, but most had plans to have one in the next twelve months. Uses to which it would be put included:
  - agency/syndicate promotion;
  - general marketing;
  - trading;
  - motor insurance issuance;
  - providing information to members' agents; and
  - marketing commercial insurance products.

- **Perceived advantages:** The main benefits from the Net were seen as being:
  - easy communication and access to risk information;
  - cheap, effective and low technology for users;
  - communication with global trading partners; and
  - access to new markets.

- **Pitfalls:** Some respondents considered the cost of Internet investment to be a disadvantage. Other perceived disadvantages included:
  - management time;
  - security concerns; and
  - capacity/speed.

Many did not understand who was funding the Internet infrastructure i.e. who was 'behind' it – the implication being that they needed to know "who was in charge".

- **Market impact on existing local networks (e.g. EPS/Linnet):** Opinions varied considerably, from those who thought the Internet would have no impact to those who believed it would have a profound effect on the development of EPS into a full-trading system. Generally, it was envisioned that the Internet would eventually improve claims and credit control.
However, the view of one respondent struck a wider chord: "In the short term, there will be a further element of confusion for the non-technical; in the medium term, this will inspire technical designers to focus on functionality and cost viewpoints as well as increasing the cadre of the technically aware. In the long term, the Internet will evolve into the preferred protocol for undertaking on-line insurance business."

London Insurance Market Network (LIMNET): LIMNET is a joint venture between LRMA, the ILU, Lloyd’s and LIBC to use technology to improve the efficiency of the London Market. They have developed a unified electronic trading system which automates the processing of claims, payment of premiums and placement of risks. On a global scale, there already exists a link between LIMNET, RINET (the European reinsurance network) and the American insurance/reinsurance networks which is intended to create international standards for electronic transmission of insurance and reinsurance information.

Looking further ahead, views again diverged. Some respondents believe that Internet technologies will become so widespread (via Microsoft products, for example) that availability will drive change. Others predicted that the Internet would fuel the existing push toward price-based commoditisation of insurance.

The picture at Lloyd’s itself is also changing rapidly. In September 1996, the Corporation launched a service with IBM which provides secure high bandwidth access to the Internet via a common gateway for all underwriters and managing agencies. By handing over responsibility for technology and security to the centre, individual agency IT departments may be able to accelerate connectivity. Lloyd’s is also developing services and content that will run across this network in conjunction with outside partners like WIRE Ltd.

Deployment among reinsurers: There is growing evidence that reinsurers are already using the Internet as an important source of material risk information.

The most active use to date has been among US property underwriters who can obtain up-to-date and detailed information on natural loss events such as windstorms, hurricanes and floods. The information is not so accessible for casualty classes, but some is available on emerging perils such as electromagnetic field and microwave risks, as well as more established classes such as personal injury, medical malpractice and environmental liabilities. Similar information is also being developed by reinsurers in London – notably AIG Europe, DP Mann Syndicate 435 and QBE.

That said, not many UK-based reinsurers have yet developed an Internet presence of their own, although Mercantile and General Re has created a detailed set of home pages providing a range of information. What is quite common is for reinsurers to allow brokers to send quotation details to their underwriters via Web-based forms. For instance, Transatlantic Re provides brokers with a facultative property worksheet which may be submitted online.
More broadly, there has been some examination by Bermudan and London-based reinsurers of the feasibility of providing reinsurance capacity information to brokers and direct buyers across the world from off-shore servers.

**Deployment by insurance and reinsurance brokers:** One of the roles of the broker is to switch information between the parties to an insurance agreement; as a result, they have most to gain — and lose — from the Internet’s applications. On the negative side they risk falling victim to the increasing commoditisation of insurance and the disintermediation that could result; on the positive side, it allows them to intermediate greater volumes of risk information across wider areas.

In spite of this, Internet deployment among UK and US brokers has been mostly limited to information-only standard home pages. Examples include Willis Corroon Group (http://www.wilcor.com), Sedgwick (http://www.sedgwick.com) and Johnson & Higgins (http://www.jh.com). Smaller brokers on the Net include Benfield's (http://www.benfield.co.uk).

An international broker which has gone a step further is the Alexander Howden Group (and its US parent Alexander & Alexander). It has established an Internet-based insurance service called Access A&A, with both a public and a private side to it: all users of the Internet can gain access to the site for information, but only those with whom Alexander Howden wants to deal are admitted to advanced functions.

**Access A&A**
4. Impact of the Internet on general and reinsurance markets

Implications for general insurers: The combination of Web-based marketing sites and EDI in an open, standardised environment could open the way to low-cost electronic trading for brokers and insurers. The deployment of cheap network computers or Web-enabled TVs would increase the potential market substantially and provide further savings.

The Internet could also provide an alternative (or an adjunct) to manned claims desks by allowing clients and brokers to get advice on claims procedures and pass on details of any third parties involved (e.g. approved repairers).

The further development of themed shopping malls on the Web (associated with focused advertising in Web-based publications, services and search facilities) will also heighten consumer awareness of the insurance services that are available. The introduction of so-called intelligent agents will enhance the usability of the Internet. There are already agents which access data sources on the Internet and collect information using previously determined rules or search patterns. Given further development and standardisation, consumers could employ intelligent agents as electronic brokers to visit insurer sites on their behalf and seek out the best prices and terms. This could have wide-reaching implications for the general insurance industry as a whole.

More generally, the development of a Web capability to handle microtransactions (i.e. very low value billing) will widen the scope for publishers of industry reports to sell material on the Internet, meaning that the diversity and quality of insurance-related information should improve. As insurance is basically an information “switching” function, this could also have wide-reaching consequences by raising consumers’ awareness of price and risk.

We believe that insurers have tended to under-estimate the potential of the Internet. For example, it is already technically possible to set up customised communication lines between insurers and corporate risk managers to improve customer service and retention, and it may happen soon.

We may also start to see a shift of Internet applications away from the mass business towards improving service for particular segments of the market – i.e. using the Internet to provide specific services to chosen clients.

Implications for brokers: The position of smaller retail insurance brokers is very different from that of the larger institutional brokers, for whom this report is primarily intended. However, it seems clear to us that insurance and reinsurance brokers alike face the threat of disintermediation. The traditional 10 per cent commission that brokers receive on all the business they handle is already under threat. Clients will use any new possibilities created by the Internet to save money by dealing directly with underwriters. For their part, underwriters resent handing over 10 per cent of their premium to brokers who take no risk, particularly at a time when technology is supposed to be reducing costs.
Insurance and reinsurance

In response, brokers are trying to protect their client base and income levels by increasing the range of value-added risk management services they offer. But their greater—and justified—concern is that the Internet could edge them out of the market altogether. Proprietary networks currently under development will eventually become compatible with the Internet and will open the way to much more direct contact between insurers and their clients. However, the Net can be a positive force as well: the brokers’ salvation could lie in the Internet’s capacity to cut the cost of shifting risk information around the world, thus enabling them to price their services more competitively.

The Internet could, therefore, strengthen the broker’s new role as an “info-mediary” who switches public and proprietary information to clients. As the insurance and reinsurance markets become more dependent upon standardised information products (such as indices), the broker could also become the supplier of the raw information upon which these new markets develop. In addition, the Internet’s ability to improve communication across markets may stimulate the development of novel risk transfer instruments and securitised products. If so, the market will become more complicated, and create demand for a redefined broking/advisory function.

In sum, the Internet could accelerate trends which are already visible in the market. If this is the case, brokers who are already re-evaluating their role—and investigating the Internet—may be able to accrue real benefits. Conversely, brokers who avoid the new technology may suffer the consequences.

Implications for reinsurers: The limited Internet-based activity among this group makes it difficult to draw more than very preliminary conclusions. However, reinsurers do not face the same threat as brokers for two reasons:

- they sit at one end of the information pipeline; and
- they actually assume risk.

Their principal function is not information “switching”, but the definition and assumption of risk. The Internet will probably allow progressive underwriters to do this more effectively and profitably—meaning that the spectrum of profit and loss within the market could widen. But how?

A progressive underwriter in 2000 may well receive historic claims data in an electronic format which could be fed directly into a rating program. His first view of a renewal presentation would therefore be in the form of a standard computer-generated rating which was ready for commercial manipulation—a system that would be far in advance of current practice. This might mean, for example, that casualty underwriters would have their social inflation factors dynamically linked to projections of tort award inflation across the world, while property underwriters could incorporate the latest changes in, say, Louisiana building codes into their decisions.

In addition, clients’ accounts-in-progress could be dynamically linked to the reinsurer from anywhere in the world and automatically monitored, making
renewal much simpler. This constant flow of high-value digital data could easily be stored, manipulated and assessed. Trends in and between accounts would be much easier to identify.

**Implications for the London insurance and reinsurance markets:**
Members of the group have suggested that the relatively unregulated nature of the Internet provides a particular opportunity for the ‘entrepreneurial’ structure of Lloyd’s.

The agenda of the New Lloyd’s, following its recent restructuring, will have to take account of Internet developments. Nevertheless, the London Market is large and diffuse, and co-ordinated action is difficult to achieve. Furthermore, the amount of investment that has already gone into proprietary systems could hinder the development of more open Internet-based services. Indeed, the dominance of proprietary systems could have negative implications for London against other insurance centres – like Bermuda.

**Implications for other reinsurance centres (e.g. Bermuda):** There has been some debate as to how the Internet might help or hinder London’s competitors, who have grown rapidly in recent years. Notable among these is Bermuda, which started as a centre for property catastrophe reinsurance and is now expanding into a wider spectrum of risks.

Bermuda’s main disadvantage has been its distance from major business producing centres. Despite this handicap, though, it has succeeded in winning a significant share of world reinsurance premiums. Skilful use of the Internet could enhance this position still further by reducing the perception of distance from customers. Furthermore, “micro-states” like Bermuda are well-placed to push through legislation to support new forms of electronic commerce that would complement the attractive tax status that they already have.

The group felt strongly that this was something that UK insurance regulators should take into consideration in any future regulatory review if the London Market is to prosper.

**Impact of the Internet**

<table>
<thead>
<tr>
<th>Institution</th>
<th>Positive Impact</th>
<th>Negative Impact</th>
<th>Leading examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brokers</td>
<td>Enhanced Information access, exchange and transfer.</td>
<td>Increased dis-intermediation</td>
<td>Access A&amp;A; Willis Corroon</td>
</tr>
<tr>
<td>Underwriters</td>
<td>Enhanced market communication and intelligence. Automated underwriting</td>
<td>Increasing division between knowledge rich/poor</td>
<td>Brockbank; Hiscox Underwriting; M&amp;G Re; Sun Alliance</td>
</tr>
<tr>
<td>Clients</td>
<td>Enhanced access to wider markets</td>
<td>None</td>
<td>N/A</td>
</tr>
<tr>
<td>London Market</td>
<td>Increased efficiency gain</td>
<td>Rise of competing electronic domiciles e.g. Bermuda</td>
<td>Artemis London Market; Lloyd’s</td>
</tr>
<tr>
<td>Ancillary groups</td>
<td>Access to information and markets.</td>
<td>Increasing competition for service provision</td>
<td>Clifford Chance</td>
</tr>
</tbody>
</table>
5. Other issues

Comparisons with the US: There are approximately 900 commercial insurance sites on the Internet – and around 600 of them are US brokers or underwriters.

There is a tendency to think that the US is driving ahead in terms of Internet applications and that the UK is following far behind. Although Internet usage is far more widespread among the US insurance community than the UK’s, this does not necessarily mean that its sophistication is also greater. US companies are not generally more advanced with respect to online trading or the creation of an online marketplace, though this could change with the deeper penetration of the Internet into the US personal and commercial markets. However, the Internet allows ideas and new products to be diffused very rapidly: consequently, applications developed in the US could quickly migrate to the UK (and vice-versa).

Insurance regulation: The working group invited a representative from the DTI’s Insurance Section to attend one of its meetings.

From the discussion, it appeared that the Department does not intend to adopt special regulations for insurance on the Internet. Officials are more concerned with the solvency of insurance companies than with the medium through which they do business. Some members of the group felt that this could prove dangerous because certain issues raised by the Internet will require specific regulatory attention (e.g. in the area of consumer protection where insurance is sold across national borders). On the other hand, the absence of specific regulation could provide encouragement to greater business activity.

Other networks: Despite the advances being made by the Internet, the world’s six largest insurance brokers recently agreed to develop a global electronic network of their own – the World-wide Insurance Network (WIN). The project’s backers are Alexander & Alexander, Aeon, Johnson & Higgins, Marsh & McLennan, Sedgwick and Willis Corroon. WIN will be available to all insurance brokers and insurance companies world-wide, and will provide what its developers say will be a more secure, customised and better managed communication system than the Internet can currently offer. Clearly, the challenge posed by WIN is considerable and will confront many insurance companies with an awkward choice. Although the two are not mutually exclusive (indeed, the plan is eventually to make WIN compatible with the Internet), it is likely that whichever system gains the upper hand will drive the other into decline.
6. Conclusion

In summary, the main findings and recommendations of the working group are:

- That the Internet is already accessible by a range of UK general and reinsurance companies. This connectivity has developed from almost nil in early 1995.

- That a significant minority of UK underwriters and brokers already has an Internet presence. The vast majority are straightforward home pages providing information only. However, a growing number of insurers' sites allow prospective clients to submit proposals to obtain quotations online. A few companies already allow policies to be purchased online.

- Despite this, there is no hard evidence – as yet – about the commercial impact that the Internet has had on insurance and reinsurance business, or on the economics of trading on-line compared to traditional means such as the telephone. More research in this area would be useful.

- The volume and sophistication of Internet applications among the UK insurance sector are increasing. The medium also appears to be gaining steadily greater acceptance among senior management.

- The Internet may have an important role in the international insurance and reinsurance community by improving electronic commerce and communications. It may also accelerate the development of hybrid products operating across markets.

- The growth of mass communication via the Internet – including voice telephony – and the development of more specific (re)insurance applications could make the Internet (or a network with similar attributes) a powerful force in the insurance markets.

- It is important to keep an eye on WIN – which, at the present time, is considered an alternative approach to the Internet. In time, the two may merge but, for now, WIN and the Internet are seen as competitive approaches to electronic trading in the insurance area.

Consequently, the group concluded that UK underwriters and brokers should not delay confronting the implications of the Internet. The potential losses from procrastination could be significant, especially *vis-à-vis* other centres such as Bermuda.
Chapter four: Equity trading

Summary: This is an area where the Net clearly has a big role. First, it levels
the playing field between big and small players, which is why so many
smaller companies are excited about Internet IPOs (though they are still
mostly hype). Second, it is cheap – and that has got full-service brokers
scared (though they are starting to fight back). Third, the equity business is
an information business and the Net is good at disseminating information,
either on a stand-alone basis or bundled in with other services. Maybe the
big stock exchanges are not yet quivering, but the US brokerage industry is
already being revolutionised by the Net – and that will spread to the UK.
One fly in the ointment: Tradepoint’s preference for Bloomberg’s proprietary
closed system over the open nature of the Net. That points to present fears
about security, speed and reliability – but even Tradepoint doesn’t rule out
Net access eventually.

Chairman: Jeff Metter Liberty (until September, 1996)
Vice-chairman: Peter Bennett Tradepoint
Rapporteur: Davide Ferrara CSFI

Working group members:

Juan Amador            Andersen Consulting
Brendan Baker          Lombard Street Research
John Bonham            Linklaters & Paines
Tomás Carruthers       ESI
Alex Fraser            Schroders
Sylvian Friederich     London School of Economics
Philip Harrison        Morgan Stanley
Tony Hobman            Proshare
Philippe Geneste       Innovative Customer Systems
Chris Lambert          ISMA Centre
Brian Scott-Quinn      Barclays Stockbrokers
Justin Urquhart Stewart Price Waterhouse
Kenneth Wilshire       Price Waterhouse
Stanley Young          Price Waterhouse
David Stewart          Price Waterhouse

The group included other members who have requested that their names not
be used. John Whitmore, of the SIB, also participated as an observer.
1. Introduction
This chapter considers the implications of the Internet and, more broadly, of HTML technologies for equity and securities trading. It aims to identify the most important ways in which the growth of Internet-based trading is likely to affect the equity trading business, looking at both threats and opportunities. It also examines the impact on stock exchanges.

This is an area where technology has already made great strides – particularly in the US, where the first initial public offering over the Internet took place in February 1996, when Spring Street Brewing – a small New York brewery, controlled by a former Wall Street lawyer – raised US$1.6 million by appealing to investors directly over the Internet. That led the owners of Spring Street to set up an investment bank, Wit Capital (named after Spring Street’s brand of beer), that, it is hoped, will develop into a full-service Internet-based investment bank.

The Spring Street/Wit Capital exercise has spawned imitations across the US, aided by a generally sympathetic SEC (which permits companies to raise a limited amount of money by selling directly to the public). But that is by no means the sum total of the Internet’s impact on equity trading. Probably far more important is the way that brokerage houses – both traditional old-line houses and new Net creations – have latched on to the Internet’s potential for cutting costs and reaching a wider range of investors. As of last May, Barron’s estimated that there were 800,000 on-line brokerage accounts in the US; now the figure is said to be around 1.2 million and one broker, Pacific Coast Brokerage (http://www.tradepbs.com/), claims 25% a month growth.

This is, therefore, one of the most exciting areas for Internet development – though it is one where the UK (and a fortiori Continental Europe) has a lot to learn from the US.

2. The drivers of change
As has already been demonstrated in the US, the Internet can be a major force for change in the way equities are traded. It can alter the business in three ways:

- **The Net can be used to disintermediate the underwriter** – allowing an equity issuer (as in the Spring Street case) to tap investors directly.

- **The Net can radically change the role of the broker** – undermining the old-line “full service” broker and even undercutting conventional discount brokers.

- **The Net is already a huge source of equity-related information** – and this is bound to reinforce the “unbundling” of such information from brokerage activity.

It is also cheap: According to Booz, Allen & Hamilton, the cost per trade of an Internet-based operation is less than one quarter of the cost of a telephone
The Internet and Financial Services

transaction, and less than one-eighth of the cost of a branch transaction.¹ That is a real driver for change.

3. The IPO market

It is easy to get carried away by the Spring Street example. It cannot be simply scaled up – not least because of serious regulatory concerns. Indeed, the Spring Street issue was in fact suspended for a while because Wit had failed to file the appropriate information with the SEC. Moreover, there have since been several cases in which state and federal prosecutors have filed charges for selling unregistered securities over the Net.

However, the fact that the SEC is generally sympathetic to Net growth and that there are individual state-regulated SCORs (small corporate offering registrations) means that lots of people are looking at cutting out the huge commissions that investment banks usually charge on IPOs. Following on from Wit Capital (http://plaza.interport.net/witbeer) are a number of other specialist US investment houses aiming to explore the world of Internet IPOs. These include Direct IPO (http://www.directipo.com) in California and Ben Ezra-Weinstein (http://benez.com) in New Mexico. There is also a Scor-Net Web site designed to exploit state programmes for direct stock issue (www.scor-net.com).

All of this can, it is claimed, tap new kinds of investor – and (a point made by Wit) can put small investors on a par with the big guys since the offer price would reflect true market demand, not a manipulated price controlled by a group of underwriters.

But how much IPO business actually takes place on the Net? There is still quite a lot of hype about bigger deals. But the main activity seems to be in raising US$1-3 million. It is, however, worth noting that there are already software companies that are offering products to automate the process of producing an Internet-ready offer document. In early 1996, there was a good deal of media attention on E*Trade – one of the major US electronic brokerage houses which announced that it was planning to do its own IPO over the Internet in June. If this had happened, it would have been a major breakthrough – but the fact is that it didn’t. Instead E*Trade ended up with a listing on NASDAQ (EGRP) following an IPO of 5,665,000 shares at US$10.50 each. This was organised along classical (non-Internet) lines with Robertson, Stephens as lead manager.

Rather than any mega-deals (the regulatory constraints of which would be enormous), the Net has stayed with small issuers or with offerings that can be accommodated under the SCOR programmes. And (however fair and democratic the Net is) the brokerage houses that have been using the Net have taken great pains to ensure that they do not get totally innocent investors. An example is IPONet (http://www.ipo-network.com/) a Web site set up by

<table>
<thead>
<tr>
<th>Exchange</th>
<th>Site address</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMEX</td>
<td><a href="http://www.amex.com">www.amex.com</a></td>
</tr>
<tr>
<td>Alberta Stock Exchange</td>
<td><a href="http://www.alberta.net">www.alberta.net</a></td>
</tr>
<tr>
<td>Amsterdam Stock Exchange</td>
<td><a href="http://www.financeweb.ase.nl">www.financeweb.ase.nl</a></td>
</tr>
<tr>
<td>Athens Stock Exchange</td>
<td><a href="http://www.ase.gr">www.ase.gr</a></td>
</tr>
<tr>
<td>Australian Stock Exchange</td>
<td><a href="http://www.asx.com.au">www.asx.com.au</a></td>
</tr>
<tr>
<td>Barcelona Stock Exchange</td>
<td><a href="http://www.borsabank.es">www.borsabank.es</a></td>
</tr>
<tr>
<td>Belgian Stock Exchange</td>
<td><a href="http://www.beurs.be">www.beurs.be</a></td>
</tr>
<tr>
<td>Bermuda Stock Exchange</td>
<td><a href="http://www.bsx.com">www.bsx.com</a></td>
</tr>
<tr>
<td>Budapest Stock Exchange</td>
<td><a href="http://www.fornax.hu/fmon/stock/betdata.html">www.fornax.hu/fmon/stock/betdata.html</a></td>
</tr>
<tr>
<td>Chicago Stock Exchange</td>
<td><a href="http://www.chicagostockex.com">www.chicagostockex.com</a></td>
</tr>
<tr>
<td>Colombo Stock Exchange</td>
<td><a href="http://www.lanka.net/fisweb/fisstock.html">www.lanka.net/fisweb/fisstock.html</a></td>
</tr>
<tr>
<td>Frankfurt Stock Exchange</td>
<td><a href="http://www.exchange.de">www.exchange.de</a></td>
</tr>
<tr>
<td>Geneva Stock Exchange</td>
<td><a href="http://www.bourse.ch">www.bourse.ch</a></td>
</tr>
<tr>
<td>Helsinki Stock Exchange</td>
<td><a href="http://www.hse.fi">www.hse.fi</a></td>
</tr>
<tr>
<td>Hong Kong Stock Exchange</td>
<td><a href="http://www.sehk.com.hk">www.sehk.com.hk</a></td>
</tr>
<tr>
<td>Jamaica Stock Exchange</td>
<td><a href="http://www.infochan.com/jamex/jam-lite/jk1-hp.htm">www.infochan.com/jamex/jam-lite/jk1-hp.htm</a></td>
</tr>
<tr>
<td>Johannesburg Stock Exchange</td>
<td><a href="http://www.jse.co.za">www.jse.co.za</a></td>
</tr>
<tr>
<td>Korean Stock Exchange</td>
<td><a href="http://www.kse.or.kr">www.kse.or.kr</a></td>
</tr>
<tr>
<td>Lisbon Stock Exchange</td>
<td><a href="http://www.bvl.pt">www.bvl.pt</a></td>
</tr>
<tr>
<td>Ljubljana Stock Exchange</td>
<td><a href="http://www.ljse.si">www.ljse.si</a></td>
</tr>
<tr>
<td>London Stock Exchange</td>
<td><a href="http://www.sels.co.uk">www.sels.co.uk</a> (not for public use)</td>
</tr>
<tr>
<td>London Stock Exchange</td>
<td><a href="http://www.londonstockex.co.uk">www.londonstockex.co.uk</a></td>
</tr>
<tr>
<td>Madrid Stock Exchange</td>
<td><a href="http://www.bolsamadrid.es">www.bolsamadrid.es</a></td>
</tr>
<tr>
<td>Milan Stock Exchange</td>
<td><a href="http://www.borsaitalia.it">www.borsaitalia.it</a></td>
</tr>
<tr>
<td>Nagoya Stock Exchange</td>
<td><a href="http://www.iiinet.or.jp/nse-jp/index-e.htm">www.iiinet.or.jp/nse-jp/index-e.htm</a></td>
</tr>
<tr>
<td>NASDAQ</td>
<td><a href="http://www.nasdaq.com">www.nasdaq.com</a></td>
</tr>
<tr>
<td>New York Stock Exchange</td>
<td><a href="http://www.nyse.com">www.nyse.com</a></td>
</tr>
<tr>
<td>New Zealand Stock Exchange</td>
<td><a href="http://www.nzse.co.nz">www.nzse.co.nz</a></td>
</tr>
<tr>
<td>Paris Stock Exchange</td>
<td><a href="http://www.bourse-de-paris.fr">www.bourse-de-paris.fr</a></td>
</tr>
<tr>
<td>Philadelphia Stock Exchange</td>
<td><a href="http://www.phlx.com">www.phlx.com</a></td>
</tr>
<tr>
<td>San Paolo Stock Exchange</td>
<td><a href="http://www.bovespa.com.br">www.bovespa.com.br</a></td>
</tr>
<tr>
<td>Santiago Stock Exchange</td>
<td><a href="http://www.bolsantiago.cl">www.bolsantiago.cl</a></td>
</tr>
<tr>
<td>Singapore Stock Exchange</td>
<td><a href="http://www.ses.com.sg">www.ses.com.sg</a></td>
</tr>
<tr>
<td>Stockholm Stock Exchange</td>
<td><a href="http://www.xxse.se">www.xxse.se</a></td>
</tr>
<tr>
<td>St. Petersburg Stock Exchange</td>
<td><a href="http://kse.spb.su">http://kse.spb.su</a></td>
</tr>
<tr>
<td>Taiwan Stock Exchange</td>
<td><a href="http://www.tse.com.tw">www.tse.com.tw</a></td>
</tr>
<tr>
<td>Thai Stock Exchange</td>
<td><a href="http://www.set.or.th">www.set.or.th</a></td>
</tr>
<tr>
<td>Tokyo Stock Exchange</td>
<td><a href="http://www.tse.or.jp/eindex.html">www.tse.or.jp/eindex.html</a> (English)</td>
</tr>
<tr>
<td>Vancouver Stock Exchange</td>
<td><a href="http://www.vese.com">www.vese.com</a></td>
</tr>
<tr>
<td>Zagreb Stock Exchange</td>
<td><a href="http://www.zse.com.hr">www.zse.com.hr</a></td>
</tr>
</tbody>
</table>
The Internet and Financial Services

WJ Gallagher & Co. In late 1996, it was posting two deals – one for Netter Digital, where it required demonstration of substantial resources before a prospectus would even be sent, and Javelin Systems, where potential investors had to attest to two years’ investment experience. The New York Times quoted IPONet’s creator as saying “this is not a place for beginners”.

4. Stock exchanges on the Net

Whether they feel threatened or not, most major exchanges are already on the Net, though their Web sites are mostly informational.

Direct trading: The most immediate threat is that the Net will enhance the ability of investors to trade existing stocks directly among themselves, without reference to an organised exchange.

Exchanges are already going on to a fully-computerised, electronic trading basis; it is easy to envisage them hooking into the Internet and there may be a demand in that many multinationals already go to considerable expense to list on several exchanges in order to ensure 24-hour trading and to broaden their investor base. The Internet, coupled with intelligent search engines, could do the same at a much lower cost.

Whichever exchange is able to offer an Internet type platform first will be in the strongest position to establish itself as the leader in this field. The biggest threat posed to stock exchanges may, therefore, be that other exchanges will make better use of the technology. The London Stock Exchange might consider this point as part of its reorganisation plans.

Will Net-based IPOs pose a threat to conventional stock exchanges? Probably not: such an approach is still fraught with difficulties, particularly for larger companies. Some of them are regulatory; some are connected with risk to the issuer; others relate to uncertainty on the part of the investor. All this makes us doubt that the practice will spread quickly. However, the technological capability exists and any movement in this direction would clearly reinforce the view that traditional intermediaries are under threat.

5. The brokerage market

Retail activity: The market for the retail brokerage industry consists mainly of private individuals, and this is where the Internet can be expected to have the greatest impact since it is essentially a medium geared to the mass market. The Internet allows retail brokers to do old things in new ways, and to offer entirely new services. But it is also forcing change on the broking industry itself through a mixture of threat and opportunity.

What kind of market is out there?: International Data Corp. of the US estimates that the number of on-line brokerage accounts in the US alone will rise to 1.5m by the year 2000 – and many people would consider that too conservative an estimate.1

Not surprisingly, many retail broking firms are already taking advantage of this to set up on-line services in both the US and the UK ranging from account management, portfolio tracking and valuation, to order placement and confirmation. This is a fast-growing area, and it is not possible to provide a comprehensive and up-to-date list of who is offering what, or where. The table below has been updated from a May 1996 issue of Barron’s, to include some offerings not primarily aimed at the US. But it only scratches the surface. There are now at least two dozen brokers offering services over the Internet and/or through ISPs like Compuserve and AOL—and competition is fierce. As a January 1997 story in the Financial Times illustrated, a small Florida broker – Empire Financial (at www.biztool.com/lowfees/) – is now offering commission-free trading for deals that meet a couple of not very onerous conditions. That in turn has forced bigger electronic brokers, including E*Trade and Datek, to cut their commissions sharply – some below US$10 per trade. Even Merrill Lynch has recently announced that it will offer Internet share trading to all its customers – which is likely to prompt a rush on to the Net by full service brokers.

There are also several Web sites that claim to offer a comprehensive range of brokerage services plus information, news, commentary and technical analysis. One such site is Herzog Heine Geduld’s PAWWS network (http://pawws.com) which carries a range of proprietary services. There is also FarSight (www.farsight.com) which provides a cheap standard platform to brokers and mutual fund operators, enabling them to put their services on-line for only a fraction of the cost of a bespoke Net site.

Electronic trading is still not an enormous market. But, as of December 1996, Barron’s claimed that a few US-based discount brokers had found that their Internet sites were accounting for over 50% of their trades – which suggests very rapid growth indeed.

**How do these Internet brokers work?** Usually the Internet component acts as the front end to an existing brokerage service (in the classical sense). Users keep an account at their chosen broker and trade it accordingly. Rather than by phone, orders are entered on-line. Holdings, account information, stock and market related information, etc. are generally also available via the Net. Some of the more advanced on-line brokerage firms also offer portfolio management software or facilities, some of which can be quite advanced, including neural network based valuation and stock selection functions. Some brokers have also integrated their Internet front end with their internal order-filling and accounting systems. It is these brokers who are reaping the most benefit from the Internet services they offer, since they are capitalising fully on the cost savings an Internet based system can provide.
<table>
<thead>
<tr>
<th>Service</th>
<th>Parent</th>
<th>Address</th>
<th>Area</th>
<th>What one can trade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ceres Securities</td>
<td>TransTerra</td>
<td><a href="http://www.ceres.com">www.ceres.com</a></td>
<td>US</td>
<td>Stocks, bonds, mutual funds and options</td>
</tr>
<tr>
<td>CMC</td>
<td>CMC</td>
<td><a href="http://www.forex-cmc.co.uk">www.forex-cmc.co.uk</a></td>
<td>World-wide</td>
<td>Currencies</td>
</tr>
<tr>
<td>eBroker</td>
<td>TransTerra</td>
<td><a href="http://www.ebroker.com">www.ebroker.com</a></td>
<td>US</td>
<td>Stocks, bonds, mutual funds and options</td>
</tr>
<tr>
<td>Electronic Share Interchange (E5)</td>
<td>ESL ltd.</td>
<td><a href="http://www.esl.co.uk">www.esl.co.uk</a></td>
<td>UK</td>
<td>Top 400 stocks on the LSE</td>
</tr>
<tr>
<td>E*Trade</td>
<td>E*Trade Group</td>
<td><a href="http://www.etrade.com">www.etrade.com</a></td>
<td>US</td>
<td>Stocks, options, futures and commodities</td>
</tr>
<tr>
<td>Fidelity Investments</td>
<td>FMR</td>
<td><a href="http://www.fld-inv.com">www.fld-inv.com</a> for Information, service is via Fidelity On-line</td>
<td>World-wide with US blogs</td>
<td>Stocks, bonds, and mutual funds</td>
</tr>
<tr>
<td>Lombard Institutional Brokerage</td>
<td>N/A</td>
<td><a href="http://www.lombard.com">www.lombard.com</a></td>
<td>US</td>
<td>Stocks, bonds, and options</td>
</tr>
<tr>
<td>Net Investor</td>
<td>Howe Barns Investments</td>
<td><a href="http://www.pawws.com/broker/How">www.pawws.com/broker/How</a></td>
<td>US</td>
<td>Stocks, bonds, mutual funds and options</td>
</tr>
<tr>
<td>Pacific Brokerage Services</td>
<td>Pacific Brokerage Services</td>
<td><a href="http://www.tradepbs.com">www.tradepbs.com</a></td>
<td>US</td>
<td>Stocks, bonds, and options</td>
</tr>
<tr>
<td>PCFN</td>
<td>Donaldson &amp; Lufkin &amp; Jennette</td>
<td>Not on Net, available via AOL (keyword PCFN) and Prodigy (jump PCFN)</td>
<td>US</td>
<td>Stocks, bonds, mutual funds and options, precious metals and options</td>
</tr>
<tr>
<td>Quick &amp; Reilly</td>
<td>Quick &amp; Reilly Group</td>
<td><a href="http://www.quick-reilly.com">www.quick-reilly.com</a> for information, Service on Computervise (GO QWKT)</td>
<td>US</td>
<td>Stocks, bonds, mutual funds and options</td>
</tr>
<tr>
<td>e.Schwab</td>
<td>Charles Schwab</td>
<td><a href="http://www.schwab.com">www.schwab.com</a></td>
<td>World-wide with US blogs</td>
<td>Stocks, bonds, mutual funds and options</td>
</tr>
<tr>
<td>Sharelink</td>
<td>Charles Schwab</td>
<td><a href="http://www.esl.co.uk/sharelink">www.esl.co.uk/sharelink</a></td>
<td>UK</td>
<td>Stocks and unit trusts</td>
</tr>
<tr>
<td>Street Smart</td>
<td>Charles Schwab</td>
<td>Via Street Smart software</td>
<td>US</td>
<td>Stocks, bonds, mutual funds and options</td>
</tr>
<tr>
<td>WealthWEB</td>
<td>TransTerra</td>
<td><a href="http://www.auflhausen.com">www.auflhausen.com</a></td>
<td>US</td>
<td>Stocks, bonds, mutual funds and options</td>
</tr>
</tbody>
</table>
Rating the e-brokers: The working group rated on-line broking services on a number of counts— including research, ease of use, products on offer and cost (1 = weak, 5 = strong):

<table>
<thead>
<tr>
<th>Service</th>
<th>Offerings</th>
<th>Ease of use</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>eBroker</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Fidelity Investments</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Pacific Brokerage Services</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Quick &amp; Relify</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>ShareLink</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Ceres Securities</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Electronic Share Interchange (ESI)</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>CMC</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>WealthWEB</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>E*Trade</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>PCFN</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>StreetSmart</td>
<td>3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Net Investor</td>
<td>4</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>eSchwab</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Lombard Institutional Brokerage</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>National Discount Brokers</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

Traditional full-service retail stockbrokers stand to lose the most from these developments because they are the most vulnerable to being bypassed. But in certain ways they also stand to gain. The key issues for them are:

- **Cost:** Before the Net, retail investors could choose between using a low cost “execution only” broker or a full-service broker whose larger commission included extras such as research. This was a fine balance, since the research was genuinely important. But now, the advent of the Net means that the retail investor can increasingly obtain high quality research for himself thanks to aids like search engines and “link” sites. Financial institutions are also making their research available on the Net as part of their marketing presence (Morgan Stanley, at http://www.ms.com, for instance, puts out reports on over 3,000 indices, 45 countries and 38 industry sectors). With all this decision-making power at his elbow, the Internet investor’s chief interest lies in executing his orders at the lowest possible cost. What, then, is the position of the full-service broker? We believe that he faces the potential loss of a large segment of his traditional market and that the market as a whole will become much more price-sensitive. In the US, the market is already large enough to support many electronic execution-only broking companies. It will take longer for Europe and Asia to reach the same level, but it seems to us that this is more a matter of when than whether.

- **Research services:** Notwithstanding the investor’s ability to find his own information on the Net, we see a need for value-added research to aid him
with his decisions. This could be supplied as an unbundled and separately-priced stockbroking service, and is a potential growth segment of the market – particularly if new means, like e-cash, become available to pay for it. A related service would be the provision of customised information on-line. As more information becomes available on the Internet, the problem will change from one of availability to one of suitability, and several companies have already been set up to repackage existing information. This is also the route taken by PAWWS – a Web site that offers a range of broking and information services, including portfolio tracking and a range of databases.

- **Pricing:** Until the arrival of the Net, retail investors had limited access to current securities prices and tick by tick movements – and little opportunity to control the timing of or the pricing of transactions. Despite the broker’s obligation of “best execution”, there is always a concern that he could have got a better price by watching market movements and news feeds and timing the deal better. Real-time price information and news systems are available but have been priced at a prohibitive level for an investor who might only deal a few times a month. The Internet allows the distribution of up-to-date prices, graphical analyses, news, etc. on a “pay as you go” basis which, together with on-line order entry, puts retail investors on the same level as professionals. The Internet can also help investors to compare prices for the same security on different markets and for other investors, allowing him to place an order to best advantage.

- **Safe custody and registration:** Investors are also concerned that their holdings are safe and that sale proceeds, stock purchases, dividend income, tax reclains, etc. are credited to their accounts correctly. Traditionally, many lodged their share certificates at their bank or kept them under a mattress. With the trend to faster settlement, there is increasing pressure to hold shares in broker’s nominee companies or in central depositories like CREST (in the UK) or the Depositary Trust Company (in the US) to avoid delays and problems in settling trades. However, many investors dislike using broker’s nominees because it prevents them from trading through another broker and runs the risk that the broker may default or even allow someone else to trade with their holdings. Internet access to broker’s nominees allows investors to check their holdings, income, etc. at any time and, if extended to central depositaries (i.e. even company registers), would allow investors to select a broker at the time of trade and to issue “electronic transfers” to authorise the release of shares to settle each transaction.

- **Customer loyalty:** The Internet is user-driven, in that a consumer chooses which pages he looks at and where he places his business. The ease of switching business means that loyalty cannot be taken for granted. Not surprisingly, therefore, service providers and software houses are striving to find ways of locking customers in. This can be done either by controlling
the products which are made available, or by creating the “magnet of convenience”.

The perception of Internet-related change is already bringing about a response from the industry.

One trend seems to be for brokers to form alliances with information providers so that they can continue to make a living once information provision has been debundled from broking. An example of this is what Q-Trade (http://www.qtrade.com) is doing. Having already signed up E*Trade, e.Schwab and AT&T Business Network as major strategic partners, it then went on to join forces with FirstCall, Disclosure, Nelsons, Valueline, Vickers and Zacks for the provision of further content. Recently it announced a further desire to link up with news providers, in an effort to provide a truly comprehensive service.

There has also been a rash of mergers in the broking industry. It would be wrong to put this all down to the Internet. Schwab’s purchase of Sharelink, for instance, mainly reflected a desire to expand outside the US. Nevertheless, these mergers are producing a potentially much more significant Internet presence, with the possibility of wider cross-selling.

That said, the Internet is not getting things all its own way. Several US brokers continue to believe that distribution via the Net remains too insecure and anarchic. They have, therefore limited themselves to closed-user intranets. The same sort of considerations appear to have swayed Tradepoint, when it decided to offer its services through Bloomberg, and not through the Internet. True, Tradepoint deals almost exclusively with the wholesale end of the market, but the concerns that weighed in its decision also weighed with other US brokers who are more comfortable off the Net.
Tradepoint: Why Bloomberg and not the Internet?

Tradepoint is a UK Recognised Investment Exchange which provides anonymous automated trading in the top 900 UK equities for professional fund managers, brokers and market makers. It is primarily a wholesale provider with average trade sizes now in the region of £350,000, though retail trades are executed on the exchange via broker/dealers. Settlement is through the London Clearing House. Its computers are accessed via a private packet-switched network with high-speed dedicated lines and PC screens operating with Microsoft Windows and proprietary software. The company plans to increase the scope of its operations by progressively adding internationally traded securities, and its reach by plugging into other global networks.

This has resulted in an agreement with Bloomberg LP as its first networking partner. Bloomberg operates a proprietary global network serving 70,000 screens and 200,000 professionals. Under the agreement, Bloomberg broadcasts Tradepoint’s market information to all its customers. Subject to regulatory considerations, traders who want to trade are able to enter orders through the Bloomberg network, and receive execution confirmation online.

Why did Tradepoint not use the Internet? Because it cannot at present meet Tradepoint’s network requirements:

- Reliable broadcast of market information in real-time: This is important because many participants continuously monitor market developments and have trading programmes which are automatically triggered when certain conditions are met.
- Encryption: To prevent unauthorised access to sensitive trading positions.
- Authentication: So that traders can be identified with absolute certainty.
- Continuous connection: So that trading opportunities are not missed.

Proprietary networks such as Bloomberg and Reuters have been designed to meet these requirements. However, the Internet is developing at a pace that will eventually qualify it for use by professionals. One of the Net’s most powerful features is its ability to interconnect and filter many information sources and bring them together on a single platform. This is important as the finance industry’s need for information is greater than any single company can satisfy.

Tradepoint does not rule out the Internet once the technical problems can be overcome – and the automated nature of the exchange fits with the Net’s capacity to carry electronic commerce. In the meantime, it uses the Net to disseminate general information about its business and provide e-mail access. Further information can be found at http://www.tradepoint.co.uk/ tradepoint

Wholesale broking: As indicated by the Tradepoint example, at present the Net plays only a small role in wholesale equity trading, mainly because it is insufficiently developed to meet the industry’s very high standards and capacity requirements. In particular, the working group identified the following problems:

- Institutional traders need real-time data on a guaranteed and continuous basis. Even though there are now companies who offer real-time feeds via the Net (e.g. DBS MarketWatch at http://rmw.dbc.com/www.html and Reuters MoneyNet at http://www.moneynet.com), the Internet continues to be subject to congestion and delays – and, as AOL’s January 1997 problems (only resolved in May) illustrate, access via ISPs can be difficult.
• The information needed by equity traders (e.g. continuously updated real-time stock prices and trading volumes) is best diffused on a single issuer to multi-subscriber basis – where the Net does not yet do as well as proprietary systems.

• On-line equity trading requires the ability to authenticate order entry and routing. This is still difficult to achieve on the Internet, though better cryptography is changing things.

• The perception of confidentiality is key in professional equity trading but it is difficult at present to achieve this to a high enough level on the Net.

However, the Internet is, even now, widely used by the wholesale market as a source of information, news, company data and so forth. It also allows traders to eavesdrop on “chat rooms” and feel the pulse of the retail investor. (There are indications in the US that chat rooms are also emerging for professionals.)

• Once the current problems (which are as much perception as fact) are resolved, the significance of the Internet for the wholesale market is likely to be its virtually limitless geographical range. This will permit institutions to reach a larger client base from a single hub, with all the associated cost savings and wider strategic choices this offers.

• A further implication of this will be to blur distinctions between consumer types. As the Internet reduces transaction costs, it will open up previously unprofitable segments of the market – the smaller corporate market and even the private investor – to the large investment banks.

6. Information and the Net
We have already noted the enormous amount of information currently available on the Net, much of it generally accessible and most (for now) free (except for connection/ISP subscription charges). But there are also some very exciting developments in the subscriber field that are worth further comment.

One is GlobalAccess – a service of Disclosure Inc. located at www.disclosure.com/disclosure – which provides Web site access to information on 13,000 US companies and 13,000 non-US firms, as well as a link to the SEC’s EDGAR filing system. Combined with a search engine, this kind of Internet-based data library can revolutionise the fund manager’s research function.

7. The future of Internet broking
Barriers to Internet take-up: The working group formed the view that the Internet is not yet being taken up as widely in the equity area as its economics suggest it should be. We therefore tried to identify barriers which could be preventing its wider acceptance.

The main one, we believe, is people's attitude to the Net – specifically unfamiliarity with the medium among potential service providers. A good illustration is the way most retail brokers process client transactions. Small transactions are less cost effective than large ones: the workload is similar but
The Internet and Financial Services

The fees are smaller. However, the greatest amount of automation occurs at the wholesale end of the market, not – as might be expected – the retail end. This failure cannot be attributed any longer to high set-up costs because these have been sharply reduced by the Internet. The truth is that these firms lack a vision of how the Internet might be exploited to rationalise their business, let alone to create new ones.

Other problems identified by the group included:

- **Security:** This is a big issue and one which is unlikely to go away in the short term, specially for the wholesale side of the industry. As discussed in Section three, the technology is not the problem, especially on the retail side where the available 40-bit encryption (and certainly 56-bit encryption which recently became exportable from the US) is probably sufficient. The real problem is one of implementation: of changing the way things are done. A further difficulty is that the threat is at present unquantifiable, making the Internet vulnerable to scare stories which the press does little to deflate.

- **Legacy systems:** Many institutions have IT infrastructure which is incapable of making effective use of HTML technology. This does not necessarily prevent them from connecting up to the Internet, but they may have difficulty integrating their operations and IT systems with Internet protocols. Meanwhile, new entrants represent the largest threat because they have the smallest legacy systems.

- **Market size:** At present, there is said to be around 650,000 Internet users in the UK but the proportion of these likely to use the Net for retail broking is tiny. The question must, therefore, arise as to whether it is worth pouring resources into this area. The same is also true on the wholesale side, where alternative systems like Reuters, Bloomberg, and Telerate already offer a higher level of information and interactivity than the Internet (albeit at a higher cost). The answer must lie in the fact that Internet use, and therefore the market it represents, is indisputably on the increase.

- **Regulation:** Almost any activity linked to equity trading is highly regulated. Any organisation wishing to use the Internet for equity trading will, therefore, have to come to terms with different regulatory regimes – not least because of the borderless nature of the Internet. The obvious regulatory and legal costs are considerable, but there may also be less obvious ones because of areas of legal uncertainty, particularly over territoriality.

- **Consumer protection:** Although linked to regulation, the group felt this deserved separate attention because of the blurring of client categories which equity trading on the Internet implies. The problem arises because specific consumer protection becomes almost impossible in an Internet context. It is therefore in the interest of the retail brokerage sector that this be resolved. The working group concluded that some sort of regulatory “seal of approval” (presumably by the SFA, IMRO or even the PIA) could
be a solution. Certification would mean that certain standards were being met, without implying any liability on the part of the certifier. Internet users would then be able to decide whether to do business with certified or non-certified sites.

The future of the Net: Clearly, there are problems that need to be addressed on both the retail and wholesale sides. Nevertheless, the group was generally optimistic that Internet take-up (already quite impressive in the US) is likely to accelerate. It noted, in particular, several new developments:

- **The FIX trading protocol**: FIX is a trading protocol that was devised in 1993 to support a connectivity project between Fidelity and Salomon Brothers. It has now been expanded to cover most trading software vendors in both New York and London – where it was introduced in mid-1996. By the end of 1997, many major institutional clients and brokers in the UK will be able to exchange order information over the Net via FIX. This is good and bad: for instance, it levels the playing field between small and big brokers, but it could undermine the role of personal relationships between brokers and clients. Nevertheless, the big institutional investors are pushing for it on the grounds that it will cut costs – and that would be a big breakthrough for the Net in the wholesale area.

- **Intelligent agents**: Major strides are being made in this area, particularly since Java allows such agents to function interactively. The assumption is that next-generation intelligent agents will drive another wedge between research and execution. An agent looks for the cheapest execution price, so a broker offering a wider service at a higher price probably will be passed over. Intelligent agents will affect the research market as well, with their ability to sort through all available sources. A well-trained intelligent agent might even be given a budget to execute a particular search or compile a market report. **One note of warning**: In 1996, Andersen Consulting demonstrated one such intelligent agent – BargainFinder, a Net search engine programmed to find the cheapest CDs for sale. As a result of the perceived competitive threat, eleven CD Internet retailers blocked its access after a few days. High cost brokerages may try the same ploy.

- **Interface development**: All speculation about Internet trading is futile if, at the end of the day, there is no market for it. That depends on access. What if the Internet became available through television screens? – an imminent prospect. One need only look at the effect that the introduction of the WWW had on the Internet to understand the importance of this. It is in this light that BT/BSkyB’s TV Internet “box” should be viewed. Such advances could dramatically alter the nature of the Internet and create huge new markets for Net-based products and services, including equity trading.

- **Welfare provision**: The driving forces behind Internet developments may also be found at a higher economic and political level. Decreasing reliance on the state for pensions means there will be more interest in personal
pensions – as there will be for private health and education, not just in the UK but in most industrialised countries. This implies greater participation in financial markets by the public and growing demand for financial services – equity trading high among them.

All of that ought to guarantee a profitable future for Internet trading, and there is certainly a lot of thought going into what could be achieved. Andersen Consulting, for instance, has a working prototype of what it calls BrokerPlus – a distribution system aimed at the wholesale market for new equity issues on a world-wide basis, using HTML technology, that would (it claims) cut administrative costs for a global book-building exercise by a factor of five from the conventional approach. Other consultancies are doing the same kind of work – as, of course, are the retail brokers, where the volume of trade is already increasing fast. Industry consensus seems to be that the next 18-24 months will be crucial. Quality of service (via ISPs) is improving, new channels (such as cable modems and interactive TV) are ready to go, and the growth of new programming languages like Java and ActiveX will make new functions possible. The assumption, therefore, is that potential players better get into the market quickly – a conclusion strongly supported by the working group.
SECTION THREE: INTERNET DRIVERS

Chapter one: Regulation

Summary: Uncertainties about regulation of the Internet are probably the biggest obstacle to its rapid take-up in the financial field. The working group is generally bullish about the Net, but it concedes that there are many areas where clarification is needed. In the meantime, some existing Internet sites may well be at legal or regulatory risk. The main areas where regulatory guidance is needed concern:
• the liability of Web sites that can be accessed in another country but are not directed at it;
• the procedures for contracting on-line;
• the formatting of electronic documents, particularly health warnings and disclaimers, and the impact that URL links and link pages can have on liability; and
• the implications of Web server location - could that affect applicable regulations?
Service providers also need to be aware of EU legislation, which may not be easily transferable to the Net, and of the complexity of UK data protection legislation (compliance with which can be hard to monitor on the Net).

Chairman: Heather Rowe
Vice-chairman: John Bonham
Rapporteur: Heather Rowe

Lovell White Durrant
Linklaters & Paines
Lovell White Durrant

Working group members:

Helen Addison
John Allanson
John Bonham
Tommaso Corrado
Henrietta De Salis
Francis de Zulueta
Elaine Hayat
Christopher Hilditch
Jeremy Robinson
Deborah Sabatot
Giles Stimson
Daniel Tunkel
David Woodall

HSBC Holdings
HSBC Holdings
Linklaters & Paines
Guildhall Ltd
Clifford Chance
Minet Group
Kleinwort Benson Investments
Simmons & Simmons
Champion Consulting
KPMG
LIFFE
Simmons & Simmons
Robson Rhodes

Martin Hollobone, from the SIB, also participated as an observer.
1. Introduction
This chapter discusses regulatory matters as they affect the Internet in the UK, with particular reference to the financial sector.

We hope to show that the Internet is not an unregulated anarchic network that financial institutions should avoid. The unique nature of the Internet as a delivery channel certainly gives rise to some problems, but these are not insurmountable; furthermore, the Internet offers opportunities for banks and financial service companies to advertise and to support electronic commerce. However, we note the lack of a legal framework for regulating the Net on an international basis, and the need to look to disparate pieces of existing legislation for national regulation. It is also important to determine what is genuinely new in the Internet, and what is not new but still requires a fresh focus.

Much of the content of this chapter is taken from notes and minutes of the meetings of the working group, as well as contributions from individual members and information from publicly available sources. It reflects the group’s understanding of the relevant regulation as at November 1996, updated where possible.

It should be stressed that this chapter is not an exhaustive analysis of regulations which could affect use of the Internet as a delivery channel. It is intended to flag certain regulatory concerns; to suggest solutions where appropriate and to stimulate debate on these issues. Where answers are evident, or options available, they are set out. Where the regulatory position is unclear, as presently it often is, the issues are highlighted and recommendations made.

Given the membership of the group, this report is written from the perspective of UK regulation, although passing mention is made of other jurisdictions.

2. Putting the Internet into context
The banking arena: Although, as noted elsewhere, three quarters of European banks plan special services over the Net, and only 14% believe that they will still have only a basic “entry level” Web site in a year’s time, over three quarters of European bank Web sites were only at entry level in mid-1996.

Nevertheless, the mantra is “Martini banking”—anytime, any place, anywhere to access your accounts. This will require much more than an entry-level Web site. The growth in bank Web sites is around 90 per cent a year in Europe, compared to a quadrupling each year in the US. However, the average growth in hits a day is 16 per cent a month. This means a doubling of hits every five months; one bank already has an average of more than 10,000 hits a day.

Structural and technological changes are closing in on traditional financial services. “Disintermediation” has become a familiar word to bankers; they are losing their clients, and they are competing with technology companies that were formerly their suppliers. As discussed below, there are certain areas where it is not even necessary to have a banking licence to supply banking services over the Internet. Banks are in danger of becoming obsolete. The Internet is both a business driver and a competitive threat, and banks should come to terms with it. Indeed, they probably have no choice.
3. New areas of concern

The Internet is simply a medium of communication, and as such is subject to many areas of law with general application. For example, a libel, breach of copyright or fraudulent misrepresentation is just as actionable when perpetrated through the Internet as it is elsewhere. Similarly, a number of activities can be carried on through the Internet that are regulated however they are carried on. Apart from the area of financial services regulation on which this report concentrates, there are other regulated activities such as gambling/lotteries.

The Internet also raises the issue of where a transaction is deemed to take place. This is relevant for two closely related reasons:

- it determines the regulatory system(s) to which a party or transaction is subject; and
- it affects the determination of which legal system governs the contractual relationship between the parties to the transaction.

However, determining the location of a cross-border transaction (and its governing law) is by no means easy. It has long been unclear exactly when an overseas firm is deemed to carry out business in the UK. One view is to apply the old legal cases which address the time and place where a contract is formed. However, these tests are somewhat technical, and the converse view (which appears to be favoured by the regulators) looks to the policy of the particular regulator. Broadly speaking, one would therefore deem a transaction to be carried out in the UK if a UK resident is the counterparty.

Complex rules of contract law relate to international contracts with a connection to more than one jurisdiction, e.g. where the party controlling the Web site is in Country A, the server is in Country B and the customer is in Country C. Even if a Web site includes an express governing law clause, the laws of the customer’s country (if that is not the same as the governing law) may have public policy rules which it can invoke to ignore even an express choice of law.

In the view of the working group, the key characteristics of the Internet which have raised new regulatory issues are:

- the ease with which it can be used for cross-border transactions involving retail investors;
- the ease with which overseas product providers can access retail investors by advertising products aimed beyond their local market; and
- the increasing use of electronic payment systems (which raises issues relating to security of payments and other transactions through the Internet).

The increased use of “electronic” documents to carry out investment transactions highlights another new feature: the use of search engines and Web indexes to help navigate through the vast amounts of information available and to sift it for what is relevant. Taken together with hypertext links, a search
engine is capable of bypassing regulatory intent, most notably when it summarises the nature and scope of sites in its own words.

Even these issues are not unique to the Internet in its narrow sense. They are applicable to any computer network, whether public (like the Internet) or closed proprietary systems such as Reuters, Bloomberg or inter-group intranets.

We acknowledge, however, that there are issues which, while not new, have assumed increased importance because of the Internet. Apart from the applicability of existing financial regulations, there is the issue of libellous material (which is much easier to publish to a wide audience through the Internet). Therefore, the practical risk of corporate liability for the acts of a careless or malicious employee is greatly increased. Indeed, corporate liability issues generally are potentially increased, so one may find oneself being proceeded against in a number of jurisdictions where the offending materials have been downloaded.

### Key regulations for UK banks

1. **Schedule 3 of the Banking Act 1987**: This sets out minimum criteria for authorisation of an institution. While much relates to qualifications of directors, it does contain some general obligations which may be relevant for the Internet, for example:
   - An institution must conduct its business in a prudent manner.
   - An institution shall not be regarded as conducting its business in a prudent manner unless it maintains adequate accounting and other records and adequate systems of control. Presumably, security and disaster recovery procedures are relevant under this category.
   - An institution must conduct its business with integrity and with appropriate professional skills. This is a broad requirement, but it could require adopting state of the art encryption systems, back-up and disaster recovery procedures.

2. **Section 39 of the Banking Act**: When a new bank is set up, the Bank of England requires that a report be prepared by an accountant - in practice, by auditors to the bank in question. This report includes a look at IT systems and disaster recovery procedures. Clearly, the Bank does not yet have the expertise to look at such functions itself, but the large accountancy firms do.

3. **BoE guidelines**: A couple of points relating to IT are raised in the Bank's Guidance Notes for applicants for authorisation under the Banking Act. Published in September 1987, these say that: "adequate controls in banks' computer and telecommunications systems are of particular importance in light of the increasing use of such technology in areas such as lending. Institutions receiving deposit-taking authority must obtain a guide to security and control in these areas from the Bank. The guide is intended to assist senior management in deciding whether their systems are sufficiently well-designed and controlled to cope with the major risks which threaten any such system."

4. **"A Guidance Note on Reporting Accountants' Reports and other Records and Internal Control Systems"**: This supervision notice was published by the BoE in April 1996. It contains a section on information technology which recognises that there are "additional risks associated with electronic environments" and that "it is the responsibility of management to understand the extent to which an institution relies upon electronic information to assess the value of that information and to establish an appropriate system of controls."
The Internet and Financial Services

**Internationalisation of the retail market:** In the field of regulation, the key novelty is the international nature of the Internet and the impact of laws:

- requiring authorisation/licences to conduct business in or into a particular jurisdiction; and
- on the issue of advertisements in that jurisdiction.

The Internet is a new way of providing cross-border services, though that in itself is not new. Many of the questions raised are essentially the same as for a firm providing services from one country into another by conventional means, such as telephone selling or mail order. What is new is the ease with which investors in one country can communicate with firms in other countries, and *vice-versa*. Investors can effectively roam from country to country without ever leaving their armchair (and without realising the legal and regulatory boundaries they are crossing) with a simple click of their mouse.

While it is not uncommon for overseas firms to sell into the UK through more conventional marketing methods, they generally need to be authorised by the UK when dealing with retail financial investors – though authorisation would not be necessary if the investor contacts the firm on an unsolicited basis. Before the advent of the Internet, it was much less common for UK investors to make unsolicited contact with firms not located in (and hence necessarily authorised in) the UK. The Internet and its associated search engines make that much more common, and call for a re-assessment of the assumptions underlying the territorial ambit of current regulation. In particular, these regulations may well be based on the tacit assumption that UK investors will generally deal only with UK firms in view of the inconvenience of dealing with a foreign firm, and that where an investor does use a foreign firm he will be well aware of what he is doing.

*This assumption must be re-assessed.*

**Electronic vs. paper-based documents:** Another area where the Internet appears to have introduced a fundamentally new issue is the manner in which information is presented and viewed. Documents presented in electronic form raise a number of issues that do not occur with paper-based documents. In particular:

- **Hypertext links can provide a path through a document for the reader to the information which he wants to read** (or which the provider wants him to read), bypassing that which is of no interest to him or which an unscrupulous provider might prefer to de-emphasise, such as health warnings. One may argue that the Internet should not require new regulation additional to that applying to paper documents. However, that proposition is justified only where there is no relevant difference between paper-based and electronic documents.

- **Hypertext links in a Web site can link to documents on other Web sites.** Conversely, other Web sites can contain links to your Web site. It is,
therefore, easy for an investor to lose sight of whose Web site he is accessing, and who, therefore, is responsible for the information provided.

- **Electronic documents are easier to browse but less easy to read in full.** Indeed, the difficulty of reading on screen and the presence of potentially side-tracking hypertext links positively discourage reading a document in full. In particular, it is more difficult to get a feel for the document overall.

- **Electronic documents are easier to update** and in practice tend to change frequently. There are evidential issues (for both user and provider) in proving what was on a Web site at a particular time. Clearly, this raises Web site “best practice” and management issues.

**Conclusion:** For the most part, the Internet does not raise fundamentally new regulatory issues. It does, however, sharpen the focus on a number of old issues. The two key factors that do call for a re-assessment of the assumptions on which current regulations are based are:

- the ease with which investors can contact firms in a different country (and *vice versa*); and

- the dematerialisation of written material and its presentation in searchable and hypertext form.

We further note the importance of recognising that certain difficult issues relevant to the Internet are not new problems but have existed unresolved for many years and merely arise here in a new context. We should not expect to see these resolved, nor should the lack of a resolution hold back the development of the Internet (any more than they have held back the international financial markets in a more conventional context).

**4. What are the main threats and opportunities?**

**Threats:** The group identified several specific issues. To start with, will there be an obligation on financial institutions to be able to recreate the exact contents of a Web page for any given day (hour, minute)? Unless they are able to do so, they may (given the dynamic nature of a Web site which will be constantly updated) be unable to prove that a complaint based upon an older version of the site is not valid. Firms will clearly need to be able to evidence ongoing compliance with regulatory requirements.

This introduces serious Web site management issues. Operational/compliance procedures may need to be in place to ensure that electronic and/or physical copies of Internet pages are stored, and that the procedure for storage is triggered by a change in the content/layout of the page. This may well have implications for Web site design.

A second point is whether the absence of clearly defined conduct of business rules in relation to the Internet allows “cowboys” to get away with practices which “good guys” have refrained from pursuing. There is a lack of certainty for conscientious members of the financial industry on what is and is not acceptable, e.g.:
The Internet and Financial Services

- what procedures should financial institutions go through to obtain regulatory clearance before establishing a Web site?

- will they have to state explicitly, on each page, which audience their Web site's products/services are directed at and provide more than minimal disclaimers to make clear e.g. what is UK-regulated and what is not? and

- if the Web server is located in e.g. Germany, but the Web site is accessible in the UK, whose rules apply and which country's regulator should take action?

In the last case, if the technology were available (which it is not at the moment, particularly given that many users access the Net through ISPs such as Demon), should financial institutions in the UK restrict access to their pages by blocking on-line enquiries with electronic addresses in (say) Germany?

A related issue is the fact that the Internet functions in an absence of geographical boundaries. This may eventually be the catalyst for promoting an international forum for regulators to resolve Internet issues. But confusion will continue until then, especially when different international regulators adopt different views in relation to use of the Internet.

Conversely, there could be the expectation of tighter regulation in relation to the Internet than currently exists with paper, because of the complex jurisdictional issues involved. There is a threat of being tempted into a technological morass which may be unnecessarily onerous in the short term.

In the group’s opinion, if there is to be more Internet regulation, it could well involve:

- a proliferation of caveats/warnings on each Web site, perhaps repeated in a footer on each page in order to combat the fact that the use of a Web browser and “bookmarks” (or knowledge of a URL) may enable a user to by-pass crucial information;

- forcing firms to print caveats/waivers/disclaimers, together with time and date stamps, should an application form/prospectus be requested by a prospective client (firms might also have to design their servers to determine whether the prospect has a printer that is on and ready to receive);

- as an alternative, obliging firms to control application/prospectus “pulling” by issuing known and potential investors with a password to the Web site page;\(^1\) and/or

- a requirement for all Internet material issued abroad by a firm to be reviewed for UK compliance by its UK arm (and for compliance in the US by its US arm, etc.)—something that would be prohibitively expensive, and that would achieve little in terms of investor protection.

---

1. This is one of the steps alluded to by the SIB to provide firms with legal certainty as set out in the letter to the chairman of the working group which is reproduced below.
It is also worth noting that current legislation does not yet take account of the use of Web browsers which will increasingly utilise intelligent agents to collect data about products which suit one's personal investment requirements. These raise serious regulatory issues of their own.

**The politics of encryption:** Governments around the world are addressing regulatory issues raised by encryption. The aim is to strike a balance between the commercial requirement for encryption and the need to prevent its abuse for criminal or other purposes.

**Opportunities:** There could be a number of opportunities flowing from use of the Internet for financial institutions and, indeed, for regulators.

Regulators (both within the UK and across jurisdictions) could take the opportunity to provide a proactive service for financial firms, resulting in the issue of interpretative guidance on permitted investment business and the Internet. This could lead them to:

- produce explicit guidelines on how to determine whether advertising on the Internet is or is not “directed” at persons in a given jurisdiction, particularly with regard to Internet material that is issued outside that jurisdiction;
- draft common health warnings or product suitability statements applicable across international boundaries/jurisdictions;
- provide generic risk warnings (or pan-jurisdictional disclosures), via e.g. a hypertext-link from a financial institution's Web pages (in the same language as the advert or application form);
- educate the public about the potential dangers of business over the Internet and help members of the public recognise those with whom they can deal (on the basis of there being some protection) and those of whom they should be wary (because they are operating outside UK regulatory jurisdiction); and/or
- establish some form of international clearing house or an internationally recognised standard, rather like a UK “kitemark”.

This could result in financial institutions willingly embracing Internet regulation, while denying opportunities to “cowboy” operators, which would be good for the industry as a whole. Such guidance could also lead to other business opportunities:

- **Digital signatures**, verified by Trusted Third Parties (TTPs), could be accepted instead of hand-written signatures. (We understand that digital signatures already have some legal standing in a number of US states; a law will shortly be in force in Germany, and a number of other jurisdictions are considering this area actively.)

- **TTPs could offer “envelope cryptography”**, where the TTP would maintain a record of who accessed what, where and when. Regulators would need
The export of encryption technology...

In 1993, the Clinton Administration proposed the Escrow Encryption Standard ("EES") containing the so-called Clipper Chip - an encryption technique which effectively contains a "back door" to enable government agencies to eavesdrop on its users. The proposal was greeted by a storm of criticism from citizen's rights lobbyists. In the UK, the export of encryption technologies (whether hardware or software) is still governed by export control regulations based on COCOM commodity control lists. However, except for France, EU member states do permit the importation and use of encryption technologies. In June 1996, the UK government published a DTI paper setting out its position on the use of encryption on public networks. This indicated that the government does not intend to regulate the private use of encryption. In common with a number of other countries, the UK has opted for a voluntary scheme in which so-called trusted third parties are licensed to provide a range of information security services to clients. In this way, commerce will be able to use secure levels of encryption whilst maintaining procedures through which intelligence and law agencies could require the disclosure of encryption keys. Implicit in the scheme is the fact that the TIP will hold sufficient information to enable the authorities to decrypt encrypted information.

The permissive nature of the UK proposals will not prevent criminals and terrorists using packages such as PGP (pretty good privacy), which are essentially uncrackable. Even if one were to outlaw the unlicensed use of such packages, the horse has already bolted with strong encryption widely available globally. In any event, would a law against the unlicensed use of encryption technology deter hardened criminals? It has been suggested that in cases involving encryption where the defendant refuses to disclose the key, the burden of proof should be shifted from the prosecution to the defendant. This route is fraught with dangers: the defendant should not be required to justify the use of encryption technologies.

Even though controversy over the Clipper Chip still rages in the US, production has commenced. As a mandatory technology under US government procurement policy, the Administration hopes that the sheer weight of government purchasing power will make Clipper Chip/EES the de facto encryption standard for telecommunications equipment. As strong crypto systems with back doors come to represent the industry norm, the general availability of truly secure crypto systems will diminish, or so the theory goes.

In May 1996, the Administration published a course of action for developing the use of crypto systems on national and international networks. Pending future government-to-government key escrow agreements, products incorporating EES technology will be exportable (as a black box) to "approved markets" (such as Europe and Australia) provided that the escrowed keys are held in the US. This raises the question as to how law enforcement and intelligence authorities in other jurisdictions will obtain access to the necessary key information to enable them to decrypt communications. The Clinton Administration envisions that future bilateral government agreements would cater for the release of escrowed keys and even the deposit on escrow of keys outside the US. In the interim, it is assumed that co-operation would be on an ad hoc basis.

Such an arrangement should be of concern to banks and financial institutions in Europe because of the high level of control it leaves in US hands. With Intelligence agencies the world over moving from political to industrial espionage, recent allegations that the US secret service hacked into the computer systems of the European Commission and European Parliament to gain knowledge of the EU's negotiating strategies during the last round of GATT negotiations will only compound such concerns and increase the need for a concerted policy to evolve in Europe.

Few European countries have implemented legislation to address the use of encryption, France being the notable exception, whilst some countries, such as Germany, have not implemented any policies at all (though Germany has legislated for the use of digital signatures). In this context, the UK government's policy paper should be applauded. However, it should not be seen as the definitive statement of the way forward in Europe. Ideally it will focus attention on the issues that surround strong encryption and foster a much-needed debate of great relevance to the future of commerce on the Internet.
to have access to such records *in extremis*, should the use of such a service become obligatory. (This could be made subject to stringent procedures, such as obtaining a judicial warrant, to ensure that access to the information could not be obtained lightly.)

- Reinforcing the culture for users to report any Web site 'breaches' etc. to an appropriate regulatory body. The SIB has already stated that it is keen to receive information about people who may be operating in the UK without authorisation.

- Reducing the need for paper copies of customer agreements by creating standards for electronic contracts (with appropriate protection for customers, perhaps by use of digital signatures).

- Reducing distribution costs, since customer agreement and prospectus information can be mailed electronically.

- Giving banks the opportunity to be TTPs – a role which, given the higher standard banks set for their own security, might well be suitable.

### 5. Areas of regulation which affect use of the Internet

**Existing financial services legislation in the UK:** The UK's prime City regulator – the Securities and Investments Board (SIB) – and the other self-regulatory organisations are in some cases still analysing their approach to the use of the Internet. However, SIB has recently issued some guidance on use of the Internet and has received responses from certain UK institutions.

In simple terms, the Financial Services Act of 1986 (FSA) prohibits an unauthorised person from issuing or causing to be issued an investment advertisement in the UK unless previously approved by an authorised person. Some material circulating on the Internet could be an investment advertisement under FSA rules if it contains an invitation or information likely to lead people to investment agreements. If so, the SIB's view is that if that information can be downloaded in the UK, it will have the right to take action against the advertiser issuing an un-approved advertisement. The point is that it is made available to persons in the UK, even if it is not primarily aimed at UK persons.

There is a carve-out in Section 207(3) of the FSA for materials published and circulated principally outside the UK. It may be worth trying to get regulators to treat the Net in this way – i.e. to claim that information on an overseas Web site which is not really intended for the UK market should be treated in a similar way to an advert in an overseas newspaper circulated principally overseas.

In regulatory terms, it is clear that an Internet Web site will frequently be an 'investment advertisement' or other form of regulated advertisement. UK law takes a territorial approach, regulating only those advertisements issued in the UK. The basic question, therefore, is whether the page is issued in the UK. However, in recognition of the fact that advertisements issued overseas may get into the hands of persons in the UK, there is a special provision deeming the territoriality problem
Dear Heather

THE FINANCIAL SERVICES ACT 1986 ("THE ACT")
THE INTERNET: ADVERTISING INTO THE UK

As I mentioned to you some weeks ago we have been considering further issues in relation to advertising over the Internet in the light of various enquiries we have received.

As Chairwoman of the CSPI Regulatory Working Group you and other members of the Group will no doubt be interested in SIB's current views on these issues.

As you know under section 57 of the Act (subject to certain exemptions and exclusions) an unauthorised person is prohibited from "issuing" or "causing to be issued" an investment advertisement in the United Kingdom unless its contents have been approved by an authorised person.

Material circulated on the Internet could fall within the definition of "an investment advertisement" in section 57(2) of the Act if it contained an invitation or information likely to lead directly or indirectly to persons entering into or offering to enter into investment agreements (such as agreements for the purchase or sale of investments or the provision of investment services).

The restrictions in section 57(1) of the Act apply where an investment advertisement is issued in the United Kingdom. It is SIB's general view that, for the purposes of the Act, where an advertisement held anywhere on the Internet is made available to or can be obtained by someone in the United Kingdom (eg it can be pulled up on a computer screen in the UK) that advertisement may be viewed as having been issued in the United Kingdom (at the point it is made available to or is pulled up on a computer screen by a person in the UK). In relation to section 57 consideration of the position of material issued outside of the UK is qualified by section 207(2) which sets
out the circumstances in which an investment issued outside the UK is to be treated as issued in the UK. This is particularly relevant to the operation of the Internet.

Broadly speaking, section 207(3) means that an advertisement issued overseas will be considered to have been issued in the UK if either it is directed at people in the UK or made available to them other than by way of a periodical published overseas and circulating principally overseas (or sound or television broadcast transmitted principally for reception outside the UK). There may be a question as to whether certain Internet material could be seen to constitute a "magazine or other periodical publication published and circulating principally outside the United Kingdom" but we consider that Internet material is not "a sound or television broadcast". In this regard much of the information on the Internet may be viewed, for the purposes of determining whether section 57 applies, as having been issued in the UK as it is made available to persons in the UK.

Whether or not any material made available to Internet users in the UK will be an investment advertisement, and, if so, whether or not its issue in the United Kingdom would constitute a breach of section 57(1) of the Act will depend on the precise facts in each case. It may be the case that one of the various exclusions within section 58 of the Act will apply.

As regards SIB's policy towards breaches of the advertising provisions and the extent to which SIB would take into account steps taken to try to avoid "issuing" an investment advertisement in the UK you may wish to be aware of the following.

By virtue of section 57(3) of the Act, contravention of section 57(1) of the Act is a criminal offence punishable on conviction by imprisonment, or a fine or both and can also form the basis of civil proceedings by SIB for injunction and restitution under section 61 of the Act. In considering such contravention SIB makes a judgement as to whether to take enforcement action taking into account the circumstances of the particular case and any other relevant factors which may include the following (please note that this is not an exhaustive list and other factors may also need to be considered on a case by case basis):

a. whether any risks to investors are such that SIB action is needed to protect their interests;

b. whether there are any other potential infringements of the Act (such as breach of section 3 of the Act) in addition to a potential section 57 breach;

c. whether as a matter of fact any offer was directed at potential UK investors;

d. the degree to which, given the nature of the Internet, someone had taken positive steps to avoid the material being made available to or receivable
by persons in the UK.

The positive steps mentioned in d above might include requiring pre-registration (before access to any potentially offending material) to ensure that only those to whom the material was aimed had access. That is not to say that such a measure of itself would mean that SIB would regard the material as not having been "issued in the UK" for the purposes of the Act. If it was in fact possible to circumvent the pre-registration or if the pre-registration was merely superficial, then clearly it would be difficult to argue that the material had not been "made available" for the purposes of section 207(3) of the Act.

It has been suggested that disclaimers saying that material was not aimed at or meant to be viewed by persons in the UK would be sufficient to avoid contravention of the Act. Clearly such a disclaimer may have the effect of putting off enquiries and, combined with a policy of refusing to deal with or on behalf of UK residents who may nevertheless access the site, would serve to reduce investor protection concerns. However, such steps of themselves do not seem sufficient to avoid the advertisements being issued in the UK if, as a matter of fact, they are received by persons in the UK.

Clearly, the Internet was not an issue when section 207(3) was drafted but SIB is looking at the implications of the effect it has in relation to Internet material. Should SIB feel that the position of advertisements on the Internet in relation to section 207(3) was a problem and one which could only be addressed by a change to the legislation it would pursue this with the Treasury. However, ultimately it is a matter for the Treasury to decide whether amendment to the legislation should be made.

SIB is not the only body with enforcement or prosecution powers under the Act, and nothing we say can be read as reflecting the views of any other agency.

Ultimately interpretation of the Act is, of course, a matter for the courts. If you have any queries about the above or, if you have any further comments to make on this issue, please do not hesitate to contact me.

I am copying this letter to Andrew Hilton and Davide Ferrara at the CSFI.

Yours sincerely,

[Signature]

Martin Hollobone
Enquiries and Investigations
Enforcement and Legal Services Division
advertisements issued outside the UK to be treated as issued in the UK if they are directed at, or made available to, UK persons.

As it stands, for the purposes of the FSA, an advertisement or other information issued outside the UK shall be treated as issued in the UK if it is directed to persons in the UK or is made available to them other than in a newspaper, journal, magazine or other periodical publication published and circulating principally outside the UK or in a sound or television broadcast transmitted principally for reception outside the UK.

We take the view that the “directed” or “made available” tests are alternatives and are not cumulative. Accordingly, an advertisement not directed to UK persons but made available to them is caught. Similarly, an advertisement directed to persons in the UK is caught, even if contained in a publication circulating principally outside the UK:

- **Directed**: Arguably, any time a UK user accesses a Web site, the information on that site is directed to a person in the UK since it is addressed and sent to his browser or his PC. We believe, however, that this is too technical an argument. In our view, to be “directed” to persons in the UK, there must either be something in the content of the advertisement which identifies it as targeted at or of interest to a class of person including UK persons, or some form of advertising of the existence of the Web site in the UK. Quotation of UK contact addresses, sterling prices or UK tax consequences might be such indications. Conversely, we would welcome guidance on whether a statement that a Web site is not directed to UK persons is likely to be of significant weight if the content of the site suggests otherwise.

- **Made available**: We note that the section refers not simply to the advertisement being available but being *made* available. There is therefore scope for argument that putting a Web site on a foreign server does not necessarily constitute the act of *making it available*. However, unless the view is taken that vetting visitors to the site is not feasible, then leaving a site “open to all” could be seen to be a positive act. We also do not believe that a Web site ceases to be “made available” to persons in the UK merely because it is also available to others – or, indeed, is primarily made available to others. Where a Web site is “accessible” from the UK, we believe it is likely that it will be regarded as “made available” in the UK. On the other hand, if password or similar protection has been built in which would prevent access from the UK, but this has been deliberately bypassed by a user, we do not believe that the Web site has been *made* available in the UK.

- **Publication**: It could be argued that an Internet Web site is really just a publication. The position on this is unclear, and open to different views. We would suggest, however, that most publications are issued at regular intervals (e.g. daily, weekly annually etc.), that each issue is separately identifiable by date and/or volume number and that most of the content changes from issue to issue. Whilst these factors could be met by an Internet Web site, most sites would be difficult to describe as publications.
The Internet and international compliance issues

Many of the problems encountered by UK Internet providers revolve around interpretation of section 207(3) of the Financial Services Act, which states: "For the purposes of this Act, an advertisement or other information issued outside the United Kingdom shall be treated as issued in the United Kingdom if it is directed to persons in the United Kingdom or is made available to them otherwise than in a newspaper, journal, magazine or other periodical publication published and circulating principally outside the United Kingdom or in a sound or television broadcast transmitted principally for reception outside the United Kingdom".

This means that any advertisement which does not fall within the exceptions listed will have to comply with all relevant UK laws and regulations. This could be interpreted as meaning that any information provided by associated companies outside the UK about non-UK investment products, would have to comply with UK regulations.

UK regulators have generally expressed the view that the Internet should not be considered as a newspaper, journal, magazine or other periodical publication, nor as a sound or television broadcast. The interpretation of s207(3) thus turns on whether an Internet advert is "made available" or "directed" at browsers in the UK. By the very nature of the Internet, advertisements are available to any person browsing the Internet anywhere in the world. Clear guidance is therefore required as to what constitutes "directed to persons in the United Kingdom". In addition:

- Is it acceptable for a site which, by advertising only authorised and recognised funds, satisfies all relevant UK laws and regulations, to have hyperlinks to or from "unauthorised" sites?
- Will the response of regulators be different if an "unauthorised" site satisfies all relevant laws and regulations in its home jurisdiction?
- Will the response be different if an "unauthorised" site is provided by an associated company of the provider of the authorised site?
- What liability rests with a site provider for links to its site from unconnected parties?

Existing bank regulation in the UK: Banks in the UK are, broadly speaking, regulated under the Banking Act 1987 – which states that no person shall accept a deposit in the UK in the course of carrying on a deposit-taking business unless the institution is authorised by the Bank of England. It is not a deposit-taking business for the purposes of the Act if the person carrying on the business does not hold himself out as accepting deposits on a day-to-day basis and if any deposits which are accepted are accepted only on particular occasions.

The result of this must be that certain types of e-cash products may escape regulation. For instance, they would not be regulated where the money they receive from customers is clearly in return for a service. Nor would they be regulated where their main business would be defined as data transmission and processing. This could be a significant advantage since compliance costs will be much higher for those providing products which require the provider to be regulated. Conversely, however, Web sites may be caught by existing regulations in several ways:
• **Advertising by banks:** So far as the UK is concerned, it will be necessary to comply, for example, with the *Banking Act 1987 (Advertisements) Regulations 1988*. These control deposit advertisements issued in the UK which contain invitations to make deposits outside the UK or any other EU Member State – i.e. they will apply in relation to deposits in the Channel Islands.

A “deposit advertisement” means any advertisement containing:

- an invitation to make a deposit; or
- information which is intended (or might reasonably be presumed to be intended) to lead to the making of a deposit.

A number of aspects of bank home pages may qualify as deposit advertisements, either because they contain a direct invitation or because they contain information which might reasonably be presumed to lead to the making of a deposit.

The requirements of the *Consumer Credit Act 1974*, in terms of credit advertisements on the Internet, need to be borne in mind when designing a Web site. The Act is clearly intended for printed materials, not for Web sites – which will require some rethinking at some stage.

• **Business prudence:** Banks must conduct business in a “prudent“ manner. This mostly relates to asset cover for their operations, but it might not be deemed prudent to enter into substantial banking transactions over the Internet unless the system is secure.

Under the same rubric, a bank must maintain adequate accounting and other records and adequate systems of control. A newcomer not providing traditional deposit-taking would not be obliged to act in this way.

**EU regulation of financial services:** Two directives are particularly relevant:

• **The Undertaking for Collective Investment in Transferable Securities (UCITS):** This creates a single market for the cross-border promotion of open-ended collective investment undertakings which invest in transferable securities and do so in a fashion which spreads investment risk. Once such a scheme is authorised in the state where its operator is based (“home state”) it may be promoted into any other member state subject to:

  - the operator notifying the host state regulator in question of his intention to promote the UCITS there and allowing two months to pass from notification for the regulator to raise objections;
  - in general, conforming to host state laws concerning marketing; and

---

1. The issues in this section are explored in more detail in an article by Daniel Tunkel entitled "The Internet and the European Single Market in Financial Services", Journal of International Banking & Financial Law, November, 1996.
The Internet and Financial Services

- more particularly, maintaining the relevant “scheme facilities” at an address in the host state.

**Unit trusts**

UK regulations for authorised unit trust schemes require the scheme particulars to be available in print. The same regime will apply from 1997 in respect of open-ended investment companies constituted in the UK. However, the form is not prescribed, merely the content. Hence, placing the scheme particulars on the Internet should not in theory be a problem. It is interesting to speculate whether UK regulations might allow a prospectus to exist on the Internet only; this depends on whether we recognise a “document” in this sort of context as including electronic representations. There are a handful of cases which suggest that the law is moving rapidly in this direction. Of course, the counter-argument is that, since many potential investors are not on the Internet, it would be unfair for the prospectus to be available only on the Internet.

A lot more can also be done over the Internet – verbal communications can pass by e-mail; documents can be exhibited on a Web site; orders to buy and sell units can be communicated electronically; and there are even ways of allowing bearer holders to identify themselves through the use of electronic passwords. The same issue of limited availability would be likely to lead regulators to require that the Internet should not be the only means by which a UCITS is promoted.

As far as marketing across borders is concerned, setting up a Web site from which it is possible to transact business is, in principle, a marketing of the UCITS into all other 17 states in the European Economic Area – and their regulators should be notified (and the Web site should not go live until two months after this notification).

Whether the UCITS can be deemed to reside at an electronic address, as opposed to a postal one, for host state purposes is not clear as far as the UK is concerned. If a statute or regulation refers to an “address”, there is some case law which suggests that it means the place where the addressee may normally be found, as opposed to an official location for him (such as a postal address). However, it would be unlikely that maintenance of an electronic address only would suffice for the purpose of UK regulations.

- **The Investment Services Directive (ISD):** The ISD provides investment firms with a basis for providing services in other EEA states, subject to a passport regime. A similar regime applies under the Second Banking Coordination Directive (2BCD) in respect of banking and investment services provided by credit institutions.

These two directives raise rather different problems. The philosophy of the ISD is that an investment firm which is authorised in its home state has the freedom to establish a branch in any host state or to offer services there. This is broadly the same for a bank under the 2BCD. It is the provision of cross-border services which is relevant for Internet purposes. All non-prudential
Regulations applicable to the branch or service are, in principle, those of the host state. Non-prudential regulations cover conduct of business, cold-calling, advertising and similar matters (as distinct from fitness and properness and capital adequacy, which are home state matters). This could create problems for selling via the Internet, since host state regulation of advertising and canvassing through a Web site implies the Web site would have to satisfy 17 different sets of regulations. Moreover, inspection of the Web site by way of compliance audit would be virtually impossible (because, once it changes, what was there before is wiped completely).

The Commission is known to be active in an attempt to resolve some of these difficulties, but nothing has emanated from Brussels as yet.

**US regulation:** A brief overview may be useful here of the regulatory issues which the US is grappling with in relation to digital cash. Like the UK, the vexed question is whether e-cash products are regulated or not.

In the US, the Federal Reserve System has significant statutory and regulatory authority with respect to consumer protection. The laws and rules it administers normally pre-empt any inconsistent state and local law or rule dealing with the same matters.

So far, e-cash has been largely unregulated in the US, although regulators and legislators are actively looking at its implications. In particular, the House Banking and Financial Services Committee’s Sub-Committee on Domestic and International Monetary Policy is looking at e-cash—concerned about its secrecy and its potential for abuse by money launderers, organised crime and terrorists.

The secrecy and non-territoriality aspects of e-cash raise bank regulatory issues in the US just as in the UK, even if the entity using the Internet is already a regulated bank (though even the definition of a bank varies from state to state). Nevertheless, account-based e-cash and home banking systems do usually involve withdrawal of deposits from conventional accounts held in institutions that are banks. Any digital banking activity is therefore likely to be attributed to the traditional bank with which it interfaces. It is much more difficult to say whether funds outside the traditional banking system, such as a digital token system, constitute banking or not. Opinions appear to be divided.

The problem of anonymity is also important. In the US, some e-cash systems require that an agency account be maintained by the service provider at a commercial bank, and that the funds remain on deposit in the banking system at all times, except when transferred over the Internet. Even if such transactions are encrypted, there is an audit trail. Other systems are not account-based and provide absolute secrecy with no audit trail. The model developed by DigiCash BV of Holland uses blind signature techniques to mask the identity of the user, and could therefore run into regulatory problems in the US. For example, regulatory authorities may find that DigiCash-type anonymous e-
The Internet and Financial Services

cash systems hamper the fight against crime, both on national and international levels.

The US already has one key piece of legislation on the books — the Electronic Fund Transfer Act of 1978 and, in particular, Regulation E which lays out the rights, liabilities and responsibilities of consumers and banks with regard to electronic fund transfers (including a requirement that financial institutions must issue receipts to customers for each transaction).

Traditional account-based e-cash or home banking systems involving a fund transfer by a traditional bank are clearly subject to Regulation E, but its application to non-banks for digital token systems is much harder to analyse. Non-banks would be subject to Regulation E if that institution “holds an account belonging to a consumer”, but it is felt that Regulation E does not apply to electronic stored-value media.

A few tentative statements have been made by US regulators. For example, the Fed has said that transfers initiated from a home computer are subject to Regulation E, but that the requirement for a written receipt does not apply. Smart cards and digital payment systems could be exempted from Regulation E by legislation but, as yet, the Fed has opposed this — though it did put forward proposals in May 1996 for amendments to Regulation E to clarify the position of stored-value cards. Its aim is to differentiate between those cards which are:

- off-line unaccountable (where the value is maintained only on the card);
- off-line accountable (where the balance of the funds is recorded on the card, but is operated with a central database); and
- on-line stored value, with on-line access to a database for the purpose of transactional authorisation and data capture.

The proposals, if adopted, would exempt systems like the Mondex card from Regulation E (because no account is involved) and would exempt off-line accountable and on-line systems from Regulation E if the maximum amount on the card at any time is no more than US$100.

6. Data protection legislation and the Internet

UK data protection: Data protection in the UK is currently regulated by the Data Protection Act 1984. The obligations under the DPA apply to data users who hold personal data about living individuals in a form which can be processed automatically in response to instructions. The DPA is most likely to apply to customer data of retail banks, rather than the wholesale market.
There are three main obligations under the DPA:

- To register with the Data Protection Registrar, which involves stating the purpose for which you are holding data and those to which you may transfer/disclose it. Breach of the obligation to register or of the legislation itself is a criminal offence, currently carrying a fine of up to £5,000 (which can be much higher if taken to a more senior court).

- To observe principles of good practice in relation to data collection, processing and disclosure. Breach of a principle is not itself a criminal offence, but the DPR can serve notice on users requiring them to take (or desist in) a particular action or not to transfer data to a particular jurisdiction. The DPR can also serve a de-registration notice.

- To give, on request, the subject of personal data a copy of data held about him/her.

The DPA is relevant to the Internet in a number of ways:

- Use of e-mail and file transfer across the Internet could mean that personal data is disclosed across national boundaries. All financial institutions should check that their registration under the DPA covers them for this.

- Banks and financial institutions may be disclosing personal data to persons not originally contemplated in their registration with the DPR, and they should check it for this.

- Data users will, by virtue of the sophisticated technology now available, be able to check vast quantities of information about individuals including how often that person visits a Web site and which sections he visited. How far does the law oblige the data user to tell the visitor that this information is being collected?

- The DPR, in its Annual Report for 1994/5, noted that members of the public may not be aware (and should be told) that Internet e-mail is not a secure medium for the transfer of data (unless properly encrypted). A financial institution setting up a Web site to which individuals can send personal data should warn them of this before the e-mail is sent. This would be similar to the warning one sees when using a Netscape browser. This warning may not be necessary for Web sites to which encrypted data can be sent.

- How financial institutions use e-mail should be carefully considered. Is it stored once sent? Is it deleted immediately? Is a hard copy printed out? All these issues may be relevant to the access requirements of the DPA, as well as for banks establishing their own corporate “best practice” in use of the Internet.

- The data protection principles must be observed – including one which says that appropriate security measures shall be taken against unauthorised access or disclosure, destruction of personal data and accidental loss. This
means that financial institutions might have to ensure appropriate use of firewalls so that personal data transmitted to a Web site cannot thereafter be accessed.

**The EU Directive on data protection:** This was adopted in October 1995 and has to be implemented by each Member State by October 1998. It bears many similarities to the DPA but in some areas goes further:¹

- The DPA regulates the processing of data, but the definition of processing is quite narrow. Under the directive, it is very wide. Processing cannot take place without the consent of the data subject, or unless the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract, or the processing is necessary for a number of other specified reasons. “Processing” means any operation which is performed upon personal data, such as collection, recording, organisation, storage, etc. This covers sending e-mail. Banks may need to look at their existing terms and conditions if they propose to use e-mail to transmit information about personal customers (however innocuous) as to whether consent should be obtained.

- The directive contains subject access provisions, and how information sent over the Internet is retained/stored is relevant to this.

- The directive contains provisions on cross-border data flows. Transfers of personal data within the EU are unrestricted, since all EU states are party to the directive which contains a high level of protection for personal data. If personal data is transferred to a non-EU jurisdiction which does not provide “adequate” protection for personal data, this is not permitted unless:
  - the individual has given his consent unambiguously to the proposed transfer; or
  - the transfer is necessary for the performance of a contract between the bank and the customer.

In practice, certain jurisdictions might be blacklisted for the purposes of data transfer, so banks might, again, revisit their standard terms and conditions to see whether consent in advance should be obtained.

The UK government completed a consultation exercise in July 1996 on implementing the directive, but we do not yet know how implementation is going to happen, or what the implementing legislation will say.

7. **Other areas of regulatory concern**

**Contracting on-line:** Contracting on-line means that an acceptance of an offer to provide products or services is communicated via the Internet, for

---

example, by e-mail or by completing an application form posted on an institution’s home page.

Where an institution advertises products or services on its home page, will this constitute an offer or just an “invitation to treat”? The significance is that if the advertising constitutes an offer, the offeror will be bound to provide such products or services should another party accept the offer. If the advertisement only constitutes an invitation to treat, the offeror will not be bound to provide such products or services. This may be important should there only be limited availability of the financial product on offer.

Communicating an acceptance to an offeror also raises difficult issues. Existing law provides the following choices:

- **The “postal rule”** deems acceptance of an offer to take place once the offeree posts his acceptance. If this rule were applied to Internet communication, it would mean that acceptance would be deemed to take place once the user has sent his e-mail – even though the company making the offer has not yet received it. This rule may not be appropriate as it was designed with a single organisation in mind which was responsible for delivery.

- **The “instantaneous communication” rule** deems acceptance to take place once it is heard or seen by the offeror over an instantaneous medium of communication, like the telephone. If this rule were applied to Internet communication, it would mean that acceptance would be deemed to take place once the company received the user’s e-mail. This rule is unlikely to be acceptable since sending e-mail via the Internet is frequently subject to delay.

- **“Chitty on Contracts”** represents an intermediate approach for communication media. The approach here is that if a sender knows (or has the means of knowing) at once whether his attempts at communication are successful, then, if he knows communication is successful, it should be deemed to be effective the moment it was sent and if he knows it to be unsuccessful, then it should be deemed not to be effective until it is actually received by the recipient. It is suggested that this principle should also apply to e-mail, EDI and financial EDI.

If this last principle were applied to e-mail communications via the Internet, it would mean that – provided the sender of an e-mail had the means of knowing at once that his message had been sent successfully and in the absence of an indication to the contrary – acceptance would be deemed to take place once the user had sent his e-mail, even though the recipient may not receive it until some time later. On the other hand, if it was apparent the message had not been sent successfully, acceptance would not be deemed to take place until the recipient had received it.

These issues may be complicated further depending upon how a company has established its presence on the Internet. It is likely that in addition to the company offering products or services to the users themselves, there may be
other entities involved – such as remote third party servers through which messages may be routed. Questions may arise as to when in fact a user does “send” his e-mail acceptance and when the recipient “receives” it. For example, receipt may take place:

- once the message arrives at the remote server;
- once it enters the recipient’s local mail box; or
- once the recipient is actually aware of the arrival of the message.

Similarly, dispatch of a message could either take place when it leaves the user’s PC or once it leaves the user’s server. When a communication is deemed to be effective is also important where revocation of any instructions is given. The same issues apply.

Clearly the position is uncertain, and financial institutions are recommended to prescribe in terms and conditions or otherwise by a notice on their Web site the method of acceptance which users must follow and set out when and how communication (and therefore acceptance or revocation) is to take place.

There is also the question of the choice of law and jurisdiction. As with any contract, it is advisable to specify the governing law which should apply and the jurisdiction whose courts and legal system are to decide any dispute. This is particularly relevant where there is any international element involved, which will frequently be the case with the Internet. An example of this might be where a US institution advertises its mutual funds (which are registered in the Cayman Islands) to investors throughout the world. The situation may be complicated further if the institution’s server is located in another jurisdiction. Failure to specify issues such as choice of law and methods of acceptance may lead to significant uncertainties.

Issues may arise as to how an institution’s standard terms may be incorporated into any contract entered into with that institution. In general, the terms that will apply to a contract will be those which are expressly agreed by the parties, together with any which may be implied by the general law. If an institution wishes to incorporate its standard terms into a contract formed via its Web page, it must ensure that any parties contracting on such terms have had sufficient notice of those terms so that they may be bound by them. This may be achieved if, for example, a user is required to click on each page – acknowledging that he has read the relevant terms and conditions.

Issues as to the contractual terms themselves may depend upon the nature of the product and services and whether or not the institution is contracting with consumers. Relevant statutes for institutions to bear in mind would include the Consumer Credit Act 1974, the Restrictive Trade Practices Act 1976, the Unfair Contract Terms Act 1977 and the Unfair Terms in Consumer Contract Regulations 1994.
Institutions should also be aware of recent cases in the English courts which have tended to overturn exclusion clauses which have been considered too aggressive. There will be risks involved in contracting over the Internet due to its unreliability in terms of speed of response; a danger of messages (including payment instructions) being intercepted and potentially altered; the breakdown of equipment; issues as to authenticating or identifying a person entering into the contract and so on. Institutions tempted to exclude liability for all or any of these risks might like to consider whether or not such an exclusion clause would be effective under current English law.

In certain cases, English statutes require contracts to be "in writing" (for instance this is the case with certain contracts to provide credit) — and the issue arises as to whether or not writing in a digital form will be acceptable for these purposes. The Interpretation Act 1988 does contain a definition of "writing" which essentially requires that it be in visible form. Whether or not words which are visible on a computer screen are sufficient for these purposes has not been considered by the courts. Similarly, issues arise as to whether or not a digital signature will be sufficient, either legally or commercially.

**Money laundering:** Increasing use of digital cash systems can cause difficulty because of the anonymous nature of some of those systems. Banks in the UK need to be able to identify their customers — the "know your customer" principle, which is vital under money laundering legislation and general regulatory controls of banking business. The Internet does not lend itself to banks being able to verify customer identity — or, indeed, in the case of e-mail, even being able to ascertain the jurisdiction from which the message has come. When opening new accounts, banks have procedures requiring them to look at hard copies of various materials to prove identity. How will this be done digitally? Clearly, very high security digital verification techniques will need to be developed before this can really be carried out without paper.

**Duties of secrecy:** Banks should also be aware of the general areas of data protection and privacy. UK banks, particularly, owe a duty of secrecy to their clients which is well established, whereas US financial institutions can make certain kinds of disclosures which cannot be made in the UK (including disclosures to associate or subsidiary firms). In the UK, there is also a law of confidence which can prevent banks disclosing confidential material without the consent of the confider. Again, the use of encryption may be relevant in order to maintain confidentiality and comply with data protection legislation.
What's going on in the EU?
The main DGs involved in the Information Society are DGXIII (telecom), DGII (industry), DGXXIV (consumer policy) and DGXV (internal market and financial services). DGIII and DGXIII both share Martin Bangemann as Commissioner and tend to cooperate. Nevertheless, each DG has a specific role:

DGXIII deals only with the truly telecom aspects (e.g. telecom liberalisation, inter-connectivity, universal service, etc.) and more technical issues (e.g. encryption). It has a considerable budget to initiate pilot studies in these areas.

DGII looks at the impact on industry. One of its Directorates specifically deals with IT and has drafted a Communication on Standardisation in the Information Society. It has an important role in G7 workshops, encouraging SMEs to become active in electronic commerce.

DGXXIV deals with consumer protection. It organised a conference, in 1996, on "The consumer in the Information Society". It has also launched a study on the consumer policy aspects of electronic payments.

DGXV deals with the financial services and transactional aspects. Its main activities are in the field of electronic payments and are reflected in the Green Paper on the Distance Selling of Financial Services. It is also involved with the regulatory framework, insofar as the problems concern barriers to cross-border service provision. Its other main activities include data protection issues. Its concern is to resist pressure for over-regulation or a re-fragmentation of the internal market by an inconsistent regulatory reaction. It has already drafted a proposal for a directive relating to Information Society services. The aim is to achieve coherence and co-operation between member states and to create an early warning system highlighting those areas where there is risk of re-fragmentation. DGXV also deals with the legal issues of encryption.

Most of the information mentioned above can be found on the Internet. The most important Web site on EU activities is the home page of the Information Society Project Office: http://www.ispo/cec.be/. Alternatively the EU's home page - with links to all aspects of EU activities - is at http://europa.eu.int/en/comm.html

8. Recommendations of the working group

Protection of genuinely "foreign" sites: The major regulatory problem posed by the Internet derives, ironically, from one of its greatest advantages: its universality. Potentially, a Web site provider must comply with all systems of law world-wide or risk enforcement action against him. These are options available to address the problem of compliance with overseas securities laws, but none is fully satisfactory.
Ensuring international compliance: At present, a firm wishing to set up an internet site has the following options to ensure regulatory compliance:

Universal compliance: Compliance with every system of law is clearly impossible. The prospect of international harmonisation is also unrealistic, given policy considerations and the large number of countries involved.

Universally recognised geographic limitation: Even if it is not possible to harmonise laws, a possibility might be to establish a universally recognised means of indicating that a particular site is intended only for persons in particular jurisdictions and that others will not be protected by the laws of their home jurisdiction.

Using technology to identify the user's location: A third approach would be to identify the location from which the Web site is being accessed, permitting access only from the countries the site is aimed at. However, our understanding is that current technology does not yet permit the user's location to be identified in every case. It is therefore not possible to block access to users accessing from outside the target jurisdictions. In principle, the technology could be developed, but current practice does not suggest this is likely. Moreover, unless regulators take significant action against a foreign Web site provider, it is unlikely that there will be a demand for it. Nevertheless, our perception is that the risk of multiple laws applying has been widely ignored: we are aware of many sites, particularly from the US, which already infringe UK investment advertising laws.

Taking the risk: Another approach is to ignore the risk of foreign enforcement action, based on an assumption that the practical difficulties of enforcement make it unlikely. Factors that might increase the comfort level of this approach include:

- **Legends/health warnings:** ensuring that the Web site clearly states that it is directed only at particular jurisdictions, that it should not be accessed from other jurisdictions or possibly that customers from another jurisdiction would not receive regulatory protection under the laws of their home state.
- **Home regulation:** ensuring that the Web site provider has a substantial and (if required) properly regulated business in the jurisdiction(s) where the site is stated to be targeted.
- **Consistency:** ensuring that the content is consistent with the assertion as to where it is directed (for example, it is unhelpful to state that a site is directed only at the US, but then to quote a London contact address and/or prices in sterling).
- **Universal standards:** ensuring that the Web site complies with standards likely to be of universal application (such as accuracy, fairness, disclosure of risks, etc.), as well as with laws of the targeted jurisdictions. It may also be prudent to ensure that the site complies with local law in all jurisdictions where the provider has a local presence.
- **Restriction of business:** ensuring that no business is done with persons located outside the stated jurisdictions unless local law has been investigated.

Password protection: For those unwilling to take the risk of foreign enforcement action for failure to comply with foreign law, the only practical available option is to block access to a Web site except to those with a password. Even this will not be safe from fraud, but the same already applies to mailing lists for sending out paper documents. A less secure variant is to require the user to sign in and to enter his name and address. Of course, this system is relatively easy for a user to bypass by inputting a known foreign address; but the user is at least making a deliberately dishonest declaration which may be regarded as depriving him of regulatory protection.
The Internet and Financial Services

Legislative amendment is necessary to ensure that reputable overseas firms are not put at risk of inadvertently breaching UK law when setting up Web sites targeted at their home jurisdiction simply because they are unable to prevent access to their sites from the UK without imposing access controls. Conversely, it is essential that the regulations remain tight enough to prevent disreputable firms setting up abroad, and ripping-off local investors through the Internet.

A regulatory solution must be implemented on a country by country basis. But in our view, the Internet should be put on a par with publications circulating primarily outside the UK – namely that they are not subject to English or Scottish law merely because they are accessible here, but will be if they are directed to persons in the UK. Any change to the legislation would require careful drafting to satisfy all interested parties.

In view of the need to maintain tight control over abuses, we do not believe that it is practicable to set out a definitive test for when a Web site is directed to persons in the UK. However, regulatory guidance would be useful as to when regulators are likely to consider a Web site to be so directed.

It may also be helpful to provide a statutory defence for a firm concerned to prove that it did not intend to deal with UK persons and had established reasonable procedures to ensure that no such persons were dealt with. At present, no formal guidance has been issued, although informal guidance is available and the SIB has been very willing to discuss issues on an individual basis with affected firms.

Regulatory guidance on format of electronic documents: The working group recommends that some (or, indeed, all) of the issues raised in relation to the format of documents on the Internet should be circulated as widely as possible, and particularly to regulators. The working group would welcome a discussion on the hypothetical situations set out in the box – with the aim of establishing "best practice" for establishing Web sites promoting financial products.

**Some hypothetical situations**

Established on a UK-based server is a site which provides detailed information about UK-authorised unit trusts managed by XYZ Limited. This site satisfies all UK laws and regulations and contains all required compliance wording. IMRO and the PIA have both confirmed informally that the advertisement does not breach their regulations. XYZ Inc. is a sister company to XYZ Limited, based in the US. It also has a Web site, although this is established on a server located in the US. The information provided there relates to XYZ Inc.'s range of SEC-registered funds. This site complies with all US securities laws and regulations - and, in fact, the SEC has provided informal confirmation that the site satisfies its advertising regulations. Now consider the following:

1. The marketing department at XYZ Ltd wishes to make use of the Internet as an advertising tool, and suggests having hypertext links between both sites. Can this be done effectively and within applicable laws and regulations?
2. The marketing department of XYZ Ltd has discovered a site created by EasIPrices Ltd., a UK based company using a UK-based server. This provides up to date prices of XYZ Ltd’s unit trusts and XYZ Inc’s SEC-registered funds, as well as listing the prices of many other investment funds and companies domiciled in jurisdictions around the world. The majority of the prices relate to funds and companies which are not authorised or regulated in the UK. Can XYZ Ltd’s site provide a hypertext link to EasIPrices Ltd’s site?

3. Having surved further, XYZ Ltd’s marketing department discovers a site it believes UK investors would find interesting. It is a site provided by a company based in Panama (MoneyGo Ltd) using a server based in Liechtenstein. This site has favourable investment reviews of all XYZ Ltd’s unit trusts, as well as XYZ Inc’s funds. The site also provides information about entrepreneurs attempting to raise seed capital - and, in particular, is promoting a businessman in Nigeria who is guaranteeing a return of 150% for investors in his rabbit farm. Can XYZ Ltd’s site provide a hypertext link to MoneyGo Ltd’s site?

4. Upon reviewing the statistics for the UK site, it becomes apparent to XYZ Ltd’s compliance department that there are a number of links from other sites to XYZ Ltd’s UK site. In particular, a number of intermediary organisations based around the world have established links to a page giving information about one of the unit trusts which has been performing well in recent months. The department needs to know if it has responsibility for browsers invited to its site.

5. The XYZ group is a multi-national organisation. The marketing teams in both the US and the UK would like to include the addresses of all 15 other members of the group, as well as a brief indication of the services provided. For the UK site, the compliance department is concerned about the reaction of UK regulators - in particular, is this making the site too international and potentially allowing individuals to gain information about unauthorised and unregulated funds?

6. Within the XYZ group, it is decided to establish an offshore site in the Cayman Islands, where the group is headquartered. From here, information about the group’s full range of funds is available - the Cayman site contains details about all the offshore investment companies and funds, as well as a hypertext link to the UK and US sites. The disclaimer wording contained on the site is to the effect that ‘if you are browsing from the UK, you shouldn’t be here but should click this button to go to our UK pages’. Human nature being what it is, investors might ignore this. Would these precautions be sufficient to satisfy UK regulators?

7. By adding a hypertext link from the UK site to the Cayman site, XYZ Ltd is aware that it is potentially giving UK individuals access to information about unauthorised, unregulated and unrecognised funds. The compliance department has drafted wording to make this clear to visitors to the UK site and to emphasise the loss of UK regulatory protection once they visit the Cayman site. By putting the onus on the browser and by making it clear that XYZ Ltd does not accept any regulatory responsibility for individuals who are browsing where they should not be, has XYZ Ltd done enough to satisfy the UK regulators?

Closer co-operation with regulators: The complex regulatory issues raised by the Internet are causing headaches for regulators and the industry alike. The working group sees these issues as an ideal opportunity for banking and financial industries and their regulators to work more closely together. The
creation of, for example, joint working parties may resolve issues more swiftly than *ad hoc* discussions. In particular, this would be helpful in establishing best practice for on-line contracting and for displaying disclaimers/health warnings.

**Location of servers:** One further area where it may be useful to clarify the legal position relates to the location of servers (i.e. the computers containing the data for the Web site). Where a firm located in country A provides a Web site which is accessed by a user in country B, one would expect that the laws of country A and B would be the only ones relevant. However, it may be that for convenience the provider locates its servers in a third country -- and, in any event, the Internet may route communications between countries A and B through countries C and D. These locations have no substantive connection with the information provided or transactions undertaken through the Internet, and it would be useful to confirm that their regulations do not need to be taken into account.

**Should the industry lobby on e-cash?** The banking industry should be calling for clarification from central banks on the extent to which existing regulation applies to e-cash, so that they can ensure compliance.

**Data protection:** Financial institutions should track the procedure for implementation of the Data Protection Directive, and respond to any consultation or green/white papers to ensure that implementation is carried out in the least intrusive way for UK financial markets.

**Digital signatures:** Careful consideration should be given to those areas where the current law in England precludes use of digital signatures (because it requires documents that are "signed" in the traditional sense), and consideration should be given to any changes in law that might be required to make use of digital signatures more widely accepted. There are a number of initiatives going on already (e.g. within the International Chamber of Commerce) which might be worthy of support.

**Contracting on-line:** Guidance should be sought as to when and where a contract is formed when using the Internet, EDI or e-mail.

**UK Web site management**

Assuming that XYZ Ltd has simply established a UK-based site for its UK authorised unit trusts, there is still debate as to the type of compliance wording which will satisfy the Financial Services Act, Banking Act etc.

It is accepted that there is a legal requirement to include certain prescribed information with any investment services advertisement; but compliance for the purposes of Internet usage may be more onerous than for a standard paper advertisement. It is seen as vital that the Internet should not be restricted in its development or discriminated against compared with other media through overzealous regulation. It is, therefore, important to raise certain issues which can be circulated widely within the relevant markets and with relevant regulators seeking "best practice" advice for compliance wording and how best to bring such wording to the attention of visitors to the site.
This is especially relevant when direct offer advertisements are considered, whereby investors purchase shares or units based solely on the information available from that advertisement. Presently, there are two information providers using the Internet to 'sell' units in their unit trusts, although both are currently restricted by Lautro rule L6.18 which requires that all such advertisements should be contained within a printed document. Both providers get around this by, to all intents and purposes, creating a direct offer advertisement on their site, then (following any application for subscription or redemption) by sending a hard copy of the scheme particulars by post as soon as practicable.

The amount of information required by a direct offer advertisement is generally considerable, and its location and provision within an Internet site is important when designing such advertisements. The questions below are applicable equally to direct offer and general investment advertisements:

- Should a compliance rubric be the first thing a visitor reads?
- Should such a rubric be available on every page?
- Most browsers will look only at what is relevant to their immediate needs – should the information be at the top or bottom of each page?
- Can there be a general page containing all of the required compliance information which browsers visit by using a hypertext link?
- Should this link be compulsory?
- Can there simply be a box which is ticked or clicked, confirming that the visitor has visited the compliance information page? Or should such a visit be compulsory?
- Is it of concern if visitors bookmark relevant pages containing investment information to avoid the necessity of re-reading compliance paragraphs?
SECTION THREE: INTERNET DRIVERS

Chapter two:
Payment and settlement systems

Summary: To realise its potential, the internet will need a payment system that works, that can cope with the micropayments that are likely to predominate in Net commerce, and that users (both buyers and sellers) can trust. At the present time, commerce over the internet is held back by the perception of insecurity. At the retail end, however, a lot of work is going on - on protocols that will increase confidence in the use of swipe cards (e.g. SET and JERI), on alternative forms of e-cash (like Mondex and Millicent) and on variants of the "trusted third party" scheme (e.g. First Virtual). At the wholesale end, the current consensus is that the role of the internet is probably going to be more important in back office and clearing support functions. However, if security and reliability issues can be resolved, the Net may also have a role to play in this area.

Co-chairman: Kathleen Tyson-Quah  KTQ Consulting
Co-chairman: Andrew Boswell  ICL
Vice-chair: Neil McEvoy  Hyperion
Rapporteur: Kathleen Tyson-Quah

Working group members:

Stephen Aitken
Dudley Bryant
Rory Cunningham
Glenda Davies
Henrietta De Salis
Chris Frost
Jonathan Herbst
Nigel Howell
Yoshitsugu Ichino
Raj Patel
Sue Roberts
Steve Sim
Rob Walker

ICL Financial Service Systems
HSBC Holdings
London Clearing House
LIBA
Clifford Chance
IBM
Simmons & Simmons
Mercury Communications
Dai-Ichi Kangyo Bank
Integral Development
Cap Gemini UK
BT
PA Consulting Group

Another representative from HSBC, as well as representatives from Edgar Dunn & Co and BACS also participated in this group. A representative from the SIB participated as an observer.
1. Introduction
Potentially the Internet has far-ranging implications for trade in goods and services. But the growth of Internet-based commerce will depend to a large extent on how easily people can pay for purchases over an electronic medium. Payment and settlement services have traditionally been supplied by banks, which makes them strong contenders to provide electronic equivalents on the Internet. But these are early days: banks have only recently begun to examine Internet issues, and their strategies in this area are still being shaped. Some of them may see commercial advantage in the area of Internet payments; others may decide that the business is not for them. These services might even be supplied by outsiders: non-banks who see this as an opportunity to get into the financial services market. There are further considerations:

- ease of access to telecom systems;
- pricing policies;
- regulatory and legislative issues;
- public attitudes toward banks and other financial service providers; and
- whether the financial sector takes up the new technology or decides to outsource transaction processing.

The starting point of this report, therefore, is that Net-specific electronic payment systems will be needed if Internet commerce is to flourish. The questions are: what form will these systems take, and who will provide them? There is also a separate question as to whether the Internet might replace existing payment systems.

Distinction between retail and wholesale payments: Payment and settlement systems are required to settle all transactions other than those involving a direct cash payment. These systems have traditionally been controlled by banks at both the retail and wholesale levels, but for the purpose of this report, the group decided to treat the two separately since they have different characteristics.

The retail payment system covers transactions in which payment is made by cash, electronic funds, plastic cards or cheques. This system relies to some extent on credit intermediary by a bank on behalf of its customers, e.g. a cheque guarantee or card authorisation which relieves the merchant of payment default risk. The users of this system tend to be merchants and private individuals.

On the wholesale side, settlement systems involve the exchange of “goods” (usually securities or currencies) for funds on a delivery-versus-payment or assured payment basis, or against a credit guarantee by a bank. Either way, the bank often plays a credit and liquidity role in settling payment obligations on behalf of a customer or an intermediary such as a broker-dealer. Users of wholesale systems tend to be financial institutions and large corporations.
The Internet and Financial Services

In both retail and wholesale payments, the banks' franchise is underpinned by the public's confidence in their integrity, their regulated status and their expertise in managing risk, liquidity and funding.

Given these advantages, it is doubtful at this stage whether their dominant position can be seriously threatened as far as conventional payments are concerned. The picture is different in the evolving Internet area, however. Although the bulk of transactions over the Net are currently being paid for by credit cards — and therefore via existing bank systems — the medium is also developing novel payment methods, and these could pose a serious challenge to banks. Quite how serious will depend on a number of factors such as:

- how far Internet commerce requires contemporaneous payment and settlement;
- the emergence of new non-bank entities providing Internet banking;
- whether banks adopt the Internet themselves as a delivery channel for traditional banking services; and
- whether the Internet can be made a sufficiently secure channel for transmitting information.

2. Retail payment and settlement on the Internet

Credit, charge and debit cards: As noted, these are currently the main forms of payment for commerce on the Internet. Instructions authorising card charges can be transmitted over the Internet with only minor modifications, though actual payments are still made via interbank systems. All other aspects of transactions remain the same: i.e.

- purchasers are still protected by statutory obligations on card issuers and suppliers;
- Visa and MasterCard-linked cards are accepted internationally (important for a medium without geographical boundaries); and
- merchants are guaranteed payment if they meet certain criteria.

From the customer's point of view, this has the advantage of familiarity, plus the usual benefits of credit facilities.

However, there are concerns linked to the use of plastic cards over the Net. These are:

- security;
- central processing costs; and
- confidentiality.

On the security issue, a buyer paying with a credit card on the Internet presently has to send his card number over telephone lines, where it is widely believed that there is a risk of interception. In fact, most card numbers are sent by some sort of secure server, and may well be encrypted — but this is not well-
known. As a result, although the risk of fraud is not Internet-specific, the perception of fraud risk on the Internet is such that many retail consumers are reluctant to part with their card details. For the same reason, banks may also provide reduced protection to merchants who deal over the Internet (as they do with telephone and mail order payments).

Fortunately, this problem is already being addressed in innovative ways. For instance, most Web browsers now have a high degree of security built into them, which facilitates the encryption of confidential information and allows it to be transmitted through secure servers. But while this may provide better security, the lack of public familiarity with such methods is hindering their acceptance. Nonetheless, the fact that these initiatives are being undertaken by non-banks should be a warning to banks that their dominance of payment and settlements may be under threat.

MasterCard and Visa have also developed the Secure Electronic Transaction (SET) protocol which is designed to make credit card payments over the Internet even more secure. SET will hide a customer’s card number from the merchant, preventing him misusing it. It requires special software and cryptographic keys to be installed on the user’s PC, which is a drawback, but chip-based smart cards using SET protocols may evolve in the near future. SET was piloted in late 1996, and is expected to become widely available in 1997. As credit cards are the main means of payment over the Net, any improvement in security should give a significant boost to Internet commerce.

The Visa & MasterCard SET standard

Prompted by concerns about the security of transactions on the Internet, MasterCard and Visa collaborated to develop a technical standard for payment-card purchases made over open networks. The new specification, SET, is a convergence of the two companies’ individual efforts. Other participants are GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems and VeriSign. SET is based on specially developed encryption technology from RSA Data Security.

Visa and MasterCard published SET specifications and began testing it in the second quarter of 1996. They expect that banks will be able to offer secure bank card services via the Internet this year. The card associations will separately test SET with consumers, merchants and financial institutions. A joint interoperability test will then be conducted to ensure that SET runs as smoothly as the point-of-sale system used today. Once tests are complete, an updated version of the specification will be published for software providers. A single standard means that consumers and merchants will be able to conduct bank card transactions in cyberspace as securely as they do in retail stores.


UUNet Pipex has also announced a system for “secure shopping” in the UK in co-operation with National Westminster Bank. “The Bureau” will provide payment processing for merchants over the Internet without requiring them to install proprietary hardware. When a customer “buys” an item from a merchant Web site and enters credit card information, UUNet will capture the details
and instruct NatWest to pay the merchant. Electronic confirmation of payment will be sent to both customer and merchant. Although there will be only a small up-front charge to the merchant for joining The Bureau, the recurring charge will apparently be 9.5% of each transaction. As this is considerably more than the average 3% charge for credit cards, The Bureau is unlikely to displace existing methods on any scale for the moment. However, its backers claim that it offers higher levels of security than over-the-counter credit card transactions and that it is superior to similar systems in the US. Over time, competition and technological advances will doubtless force these charges down.

On top of that, Netscape—also hedging its bets—teamed up with CyberCash in October 1996 to offer the latter’s CyberCoin payment system with its own browser software called Netscape Live Payment.

A comprehensive approach to Internet commerce: Banks beware

UUNet Pipex, Europe’s largest ISP, has launched DialStore. Located at http://www.bureau.pipecom/merchant/dialstore.html, DialStore allows people who wish to sell on-line to build their Web site ‘shop’ using the 1Mb of free Web space with their PIPEC Dial account, and then ‘commerce-enable’ the store using The Bureau for a one-off fee of £500. The result is a 24-hour, global retail store accepting Visa and MasterCard, with NatWest as the clearing bank. The Bureau manages all stages of the transaction from browsing around the store and collecting items to online processing of the credit or debit card payments and statements for both merchant and customer. The proceeds from sales generated by the store are delivered to the vendor in monthly payments. If the merchandise is a ‘soft good’ such as software or information, The Bureau will automatically deliver the merchandise over the internet.

A further consideration is the development of alternative “micropayment systems” using e-cash to facilitate the growth of small value commerce on the Internet. Nonetheless, without significant volumes to justify lower charges and better links to core processing systems, card issuers and service providers appear unwilling in present to reduce their fees for Internet commerce.

As far as processing is concerned, some US Internet users are now developing electronic payment systems which transmit instructions via the Internet to banks to debit a customer’s, or credit a merchant’s, account – just like cheques or EFTPOS. To succeed, however, such systems will need a significant central processing infrastructure much like plastic cards, a critical mass of users, and adequate security levels. Unless they evolve from conventional systems (such

1. Transaction charges for credit cards are usually in the range of 3 to 5 per cent, although large retailers can negotiate this down below 2 per cent. Fees for debit cards are calculated on a per transaction basis. Even these charges can put pressure on merchant margins.

2. The 1996 survey by Booz, Allen & Hamilton indicated that costs associated with Internet non-cash transactions were substantially lower than for all other payments. The unit costs were US$0.15 for an Internet payment, US$0.26 for a PC banking payment, US$0.54 for telephone banking, and US$1.08 for a branch transaction.
as BACS in the UK), they are unlikely to have much advantage over existing payment methods, particularly for small value transactions.

The JEDI standard: The World Wide Web Consortium (W3C) and CommerceNet have established specifications for a Joint Electronic Payments Initiative (JEDI). This provides a universal payment platform that allows merchants and consumers to transact business over the Internet using many different forms of payment. W3C and CommerceNet have developed JEDI specifications with industry leaders, including Microsoft, IBM, CyberCash, Xerox, British Telecom and Digital who are all implementing the Internet payment protocol in their systems.

Since merchants accept different forms of payment, the Internet needs a standard through which these can all be channelled, and connectivity to a wide range of banks, counterparts, etc. can be achieved. JEDI is a standard mechanism for Web clients and servers to negotiate payment instruments, protocols, and transport between one another. It consists of two parts:

- an extension layer that "sits" on top of http - the Protocol Extensions Protocol (PEP) and
- the Universal Payment Preamble (UPP), the negotiations protocol that identifies appropriate payment methodology.

Those protocols make payment negotiations automatic for end users. As a result of feedback from the initial project, the second phase (beginning in early 1997) will:

- encompass a larger number of payment systems, including direct billing systems, electronic cash, micropayment and electronic checks;
- incorporate hardware security tokens (smart cards or PCMCIA cards);
- establish common APIs; and
- involve a larger number of European and Japanese financial service companies to allow for input from users of the technology (in addition to the creators).

Tim Berners-Lee, creator of the Web and now a director of W3C said that one of the ingredients needed for Web commerce is the ability for different payment protocols to exchange information. JEDI addresses this need.

More information can be found at http://www.w3.org/pub/www/payments or at http://www.commerce.net.

Electronic cash and micropayments: Electronic "purses" have several promising features for Internet commerce.

These were initially developed separately from the Internet for small-value transactions such as parking, public transport and telephones. The mechanism is typically a "smart card" able to store and transfer units of value, and to be replenished through special hardware installed with merchants, banks and telephones. In an Internet environment, the purse could be stored on the hard drive of a PC or on a swipe or chip card which interfaces with a PC through a card reader. DigiCash is the only electronic purse currently linked to the Internet in the UK, but several other systems are examining this possibility. Mondex, the most highly developed electronic purse scheme in the UK, does not currently extend to the Internet, though it plans to do so.
**Mondex Internet transactions:** Purchases on the internet are widely forecast to exceed US$200bn by 2000, and most will be less than US$10. This creates a need for secure payment methods which are as simple as the traditional ones. While Mondex was primarily designed as an alternative to physical cash, it can also offer the Internet user a way of paying in the virtual marketplace.

Currently, around 45 per cent of physical transactions are between about US$1.50 and US$7.50. But ISPs are taking or sharing just frans of a cent for access to their pages; so the proportion of ‘micro-transactions’ over the Internet is likely to be much higher than in the physical cash world. The high costs of centrally-accounted systems (like credit cards) rule them out as payment mechanisms for such tiny sums. But Mondex — where everything takes place at the level of the chip in the card — reduces the marginal cost of a transaction to virtually zero. With Mondex, therefore, transactions of even one cent (or one penny) become viable.

Mondex’s security relies on a unique ‘digital signature’ generated by an on-card chip which can be recognised by the other Mondex card involved in the transaction. This signature is the guarantee that the cards involved are genuine, and that they are dealing with unaltered Mondex signals. This recognition process also identifies the counterparty card for which the cash is intended — so funds cannot be intercepted by a third party without detection.

A Mondex transaction on the Internet might look like this:

1. Having reached the on-line site or mail that accepts Mondex, the user browses and selects his purchase.
2. On completion of the selection (and confirmation to the vendor), he inserts his Mondex card into a card reader attached to a computer.
3. On confirmation that another valid Mondex device exists at the other end of the link, value is transferred from user to vendor in the preferred currency.
4. Electronic goods are downloaded to the user immediately, while physical goods are delivered by traditional means.

Mondex prototypes are currently being tested on the Internet by Mondex franchisees and supplier companies. Further announcements are expected over the next 12 months.

Electronic cash – digital units which are redeemable for currency – will be the Internet’s equivalent of specie money. However, the economics of electronic cash schemes depend to a great extent on whether they are “accounted” or “unaccounted”:

- **An accounted** scheme is basically a “spoke-and-hub” system, which requires a central record-keeper (like a bank) to process transactions and keep track of transfers of e-cash among users, rather like using cheques or debit cards with existing bank accounts. Although it is the most common system, it can be expensive to run. It is, however, good for banks, who are well placed to earn fee income as the third party involved in all transactions.

- **An unaccounted** (or direct) scheme treats e-cash exactly as real cash, with transfers moving directly from purse to purse, without intermediation or record-keeping. This system is much cheaper for both seller and purchaser. As a result, although it is much less common today than the “spoke-and-hub” approach, it is expected to prevail in the longer term.
With unaccounted e-cash, the units themselves represent the store of value, and an Internet message can effect their transfer from one purse to another. There are no service charges for transferring e-cash and no centralised record of transactions, which makes e-cash particularly suitable for small value transactions. The units can be instantly reused by the receiving purse holder, which eliminates credit risk for merchants and intermediaries and permits freer commerce among participants in the system. The risk of fraudulent interception of an e-cash payment is limited to the value of that payment. It is, for all practical purposes, cash in an electronic form.

Units of electronic cash may also be redeemed in multiple currencies, depending on the terms of the issuer. This should facilitate cross-border commerce in an environment like the Internet which is unconstrained by geography.

The biggest challenge to the development of electronic purses is the achievement of critical mass: a sufficient number of consumers and merchants must accept electronic cash to make a system worthwhile. As yet, no dominant system has emerged, though given the high stakes and the likelihood of a “winner takes all” outcome, developments may be rapid. It is noteworthy that MasterCard recently bought into Mondex, despite its endorsement of the SET-based approach it helped pioneer.

An alternative approach to the problem of micropayments is being pioneered by Digital, which is now trialling its Millicent system. This is specifically targeted at payments of a fraction of a cent. It gets around the economics of this by using “distributed brokers” who sell scrip to end-users and then pay the information providers. Such brokers may well be banks.

A particular concern with e-cash is the need for confidence in the issuer since the soundness of such a system ultimately depends on its remaining in business. The electronic purse schemes operated in the UK by Mondex and DigiCash are both backed by banks.\(^1\) While this does not provide a total guarantee (because even banks can become insolvent), it gives users a measure of comfort. Future schemes might be run by unregulated entities, in which case holders would have to form their own judgements about their soundness.

Some commentators have pointed out that major corporations might make better issuers than banks (or even sovereign entities) because of their stronger credit standing, so that if Microsoft issued e-cash, people might prefer to hold “Bill’s dollars” rather than dollar bills. Predictably perhaps, a report by the Bank for International Settlements (the “central bankers’ central bank”), which included a special Annex on the Internet, implicitly recommends that only banks should be authorised to issue e-cash.\(^2\)

---

1. Whether the issuance of e-cash constitutes acceptance of a deposit under the laws of any given jurisdiction will depend upon how any particular scheme is structured; in the UK, only authorised banks may accept deposits in the course of a deposit-taking business.

Private currencies are on the way: With the advent of cyber-currency comes the possibility of currencies other than those issued by national central banks – a development predicted in a CSFI paper by Edward de Bono three years ago. Embryonic private currencies already exist in the form of customer loyalty schemes operated by large corporations (such as air miles and talking points). These could evolve into claims on those corporations’ revenues. E-cash technology would provide the means for these currencies to become convertible into each other, and to circulate more widely.

Acceptability is the greatest barrier to the expansion of alternative currencies. All that prevents Shell points from being tendered for goods other than at Shell stations is the willingness of people to take them. Cash is acceptable to all because it is easy to authenticate and is backed by a central bank. However, electronic commerce and instantaneous communication would permit automatic authentication of alternative currencies – thereby strengthening people’s faith in them. This could open the door to a host of "private" currencies issued by corporations or even individuals.


A final point. Plastic card purchases all involve capturing information about the transaction, which some customers may like, others not. One of the attractions of e-cash is that it need leave no trace as it flashes from chip to chip, rather like money passing from hand to hand. Is this a good thing? It depends on how society weighs the competing interests of privacy and wider social concerns.

Multi-currency payment systems: There is already great interest in multi-currency payment processing to support Internet commerce. The market for products delivered in bits rather than atoms, transported by satellite rather than ships, is not geographically restricted. Merchants can offer their wares via their Web sites to customers world-wide, with no additional cost for marketing across borders (other than a possible increase in legal and compliance costs). Indeed, a great deal of software – for entertainment, education and personal financial management (eg. Quicken) – can already be bought cross-border over the Internet, even though the customs duty implications may not have been fully worked out.

One potential benefit offered by e-cash or Internet payment systems is improved cross-border payment processing in multiple currencies, which will appeal to retail customers and small businesses who are frustrated by the cost and delays of existing cross border systems. E-cash units which are readily redeemable in several currencies at low cost would draw many more retail and commercial users to the Internet.

3. Wholesale payment and settlement systems
Most high-value payment and settlement systems in the UK are proprietary networks owned by banks (e.g. CHAPS, CrestCo, the Central Gilts Office, SWIFT, ECHO, LCH). The close control which banks exert over these systems is intended to protect them from fraud and abuse, but it also helps to preserve the banks’ unique franchise in processing high-value transactions.
Payment and Settlement Systems

At this time, we have no knowledge of firm plans to open up any high value payment or settlement system to Internet access although several institutions are known to be exploring the application of HTML technology to the development or extension of existing systems via intranets or private networks.

**Back office and clearing support functions:** The Internet may have a more immediate relevance to the wholesale market in the area of back office administration of payments and settlements.

An early use of the technology might be for institutional investors or remote bank branches to confirm foreign exchange or securities trades. The restricted access given to most payment and settlement systems forces market participants to funnel their payment instructions through tiers of intermediaries. If they can send details more directly, the risks associated with settlement—and therefore the cost—should be reduced. The case with which the Internet can transfer complex data among multiple users could therefore produce a rapid improvement in the processing of international wholesale financial transactions. The Depository Trust Company, the settlement system for trades in US equities and corporate bonds, has already announced beta testing of Internet trade confirmation processing for institutional investors which, if successful, promises significant cost savings.

The Internet may also provide a means of electronic data interchange between businesses. For example, the Royal Bank of Scotland and PNC Bank (in the US) have announced the development of a bilateral EDI service for customers of the two banks which will enable them to make rapid and efficient cross-border commercial settlements using the EDIFACT standard. This is believed to be the first multi-currency EDI service which fully meets EDIFACT standards.

4. **New issues in payment and settlement systems arising from the Internet**

Most UK banks have, so far, only explored the Internet’s potential for marketing existing products and services, rather than its wider possibilities. Relatively few of their Web sites are fully interactive, although most banks expect to offer more services via the Net in the years ahead. Electronic “shopping malls” (such as BarclaySquare and Buckingham Gate) have been promoted as a means of selling services and obtaining customer information, but so far they have not proved very successful for the non-bank merchants who use them.

All these initiatives need to be backed by payment and settlement systems. As pressure to provide more comprehensive Internet services increases, the demand for such systems will intensify. We therefore envisage that the payment and settlement area will become one of the most competitive on the Internet—and that competition, involving banks and non-banks, will drive innovation.

This is also the case with intranets. Several banks and service providers already offer financial market information and risk management services on-line. The
The Internet and Financial Services

publication of information about market prices and conditions on the Internet—especially when combined with proprietary software—can greatly extend the access of investors and treasury managers to real-time trading. Electronic market information can be distributed efficiently to all potential market participants with little additional cost. Any usage charges will, however, require corresponding payment and settlement systems able to support the instantaneous and on-line nature of the medium. For example, Barclays is developing an Internet site for real-time access to London Stock Exchange prices, aimed at eventual direct trading. This would not only significantly increase competition for the provision of such services, but would require comprehensive settlement arrangements to be established.

It seems likely, therefore, that the provision of new and increasingly comprehensive on-line services will fuel competition in payment and settlement systems.

Risk management, scenario analysis and stress testing are also services being offered to wholesale market participants via the Internet by companies like Integral Development Corp. (http://www.integral.com) Not every institution can afford complex proprietary systems for measuring risk and capital adequacy requirements on changing portfolios of traded instruments. Remote risk management services can now offer to take encrypted portfolio information via the Internet and re-deliver the processed information by the same means—again extending access to high value added services to a much broader cross-section of market participants than would have been conceivable a few years ago.

5. Opportunities and threats for the banking and payment sectors

Although the Internet opens the way to new forms of intermediation and new efficiencies in the transmission and processing of complex information, it may also have a negative impact on existing providers by:

- splitting the banking industry into those who can adapt to new technology and those who cannot;
- leading to the disintermediation of banks, as new entrants claim part of the traditional banking franchise; and
- hastening concentration in the banking sector.

Banks, therefore, need to ask themselves some tough questions about the Internet:

- where/what is their “added value” in the transaction chain?
- how can they ensure that their franchise in facilitating or processing payments and settlements will last? and
- how strong is their ability to compete with non-bank developers of the infrastructure for Internet commerce?
Potential for concentration and tiering in the banking sector: Banks have several traditional strengths, in particular:

- in-house risk management skills;
- their status as regulated protectors of depositor’s funds; and
- access to inter-bank credit and central bank liquidity.

These strengths will remain relevant in an Internet environment since banks will need to retain credibility if they are to authenticate payment instructions, verify availability of funds or credit, guarantee payments, and process large volumes of low value transactions. However, the speed at which the Internet operates means that the banks may lose control of the “float” and other sources of income that exist in more leisurely traditional systems. Internet depositors and merchants will demand greater control over cash flow and more efficient processing of payments than is expected for cheques and cards, which will reduce the float of customer cash. Although transaction fees may not be immediately affected, banks are at risk of losing these to low-cost non-bank providers over time.

The First Virtual Internet payment system
First Virtual Holdings Inc. (of San Diego) has established an innovative system to provide a simple and secure method for buying and selling over the Internet. No special hardware, software or encryption is required, only ordinary e-mail. In practice, FV offers itself as a third party repository for sensitive information. It issues clients with a Virtual PIN (an alias for individual credit card information) to make purchases. Credit card numbers are therefore never transmitted over the Internet. As added security, every purchase made at any cyber-shop accepting this form of payment is confirmed via e-mail.

As a result, the front-end (what concerns the user) is extremely simple. To obtain a Virtual PIN one needs only have Internet e-mail and a valid credit card. Upon completion of an application - the sensitive parts of which can be sent in by mail, given over the telephone or relayed via a secure server - a Virtual PIN is issued (again through a secure method). Once registered, the user need only give the Virtual PIN to a seller whenever a purchase is made. Purchases are then automatically confirmed via e-mail from First Virtual. This requires a confirmatory “yes” to be returned by the user to the bank to complete the sale. A “no” results in the immediate cancellation of the transaction. Once the sale is confirmed, the user’s credit card is charged by First Virtual off-line and the proceeds credited to the retailer.

This payment method is simple, secure and innovative - assuming one trusts First Virtual. Since the process is easily automated, it is also very cheap: the annual fee is US$2.00. It is also cost-effective for the merchant since he does not have to register or buy new hardware.

More information is available at http://www.fv.com

Concentration has been occurring in the banking sector for the past decade, even without the Internet. However, the Net is likely to reinforce the trend because the cost base for Internet banking is substantially lower than for branch banking.
The Internet and Financial Services

The pressure will be felt most keenly by banks with large branch networks as these have much higher cost-to-transaction ratios. Again, the ability of the investor to access complex information through the Internet may undercut any advantage held by local branches. If face-to-face interaction is required, it can be provided by IFAs or via Internet teleconferencing. Established banks may also suffer relative to virtual banks in having to reconcile Internet banking systems with legacy systems connecting their branch networks.

The Internet also changes traditional commerce by speeding up and blurring the steps involved in a transaction. A normal transaction in the real economy would consist of:

- a buyer’s request for quotes;
- a review of the preferred vendor’s goods or service;
- placing of an order;
- payment; and
- delivery of goods.

With virtual commerce, all these steps can occur in a matter of seconds. Moreover, merchants may extend their role to include financing customer purchases or facilitating payments through proprietary charge card schemes. Banks will continue to have a role in payment authorisations, volume processing and bulk settlement; but such functions are low-value and low-profile relative to the position of the merchant with the customer. This could have a considerable impact on the future place of banks in the payment value chain.

**Branding:** Banks benefit from a strong public brand image for providing security and for customer service. This may be more important in the Internet environment than it is on the high street. To the extent that customers continue to rely on their banks for advice in making longer term investment and banking decisions – such as pensions or mortgages – they could prove as loyal to their bank’s Web site as to the corner branch. Banks may try to reinforce this customer loyalty by making more effective use of their customers’ account histories to improve profiling and provide better targeted services.

Digital certification of parties to an electronic transaction may provide another opportunity for banks to use their reputation for trust and integrity. Certification uses encryption and a central register to verify the identity of a merchant or customer prior to a transaction. Banks may thus interpose themselves as “trusted third party” guarantors in promoting Internet commerce, in addition to providing online payments. Certification would greatly enhance the appeal of online payments processing; as a result, several vendors are already developing certification methods consistent with the SET protocol.

One opportunity for banks presented by data capture in an Internet environment is the sophisticated analysis of consumer buying patterns and behaviour to support cross-selling. If banks are displaced from retail payments, they could
still move to the cross-selling of other financial products. Alternatively, if banks continue to play a central role in processing payments for Internet commerce, they may gain a wider insight into the behaviour of their customers at little additional cost. In fact, the market information thrown up by a transaction may be more valuable than the settlement fee it generates.

6. Public policy implications of Internet-based payment and settlement systems

The Internet's lack of operational and geographical limitations poses a challenge to government authority in many areas, including regulation, enforcement, monetary policy and tax. With bytes replacing documents in international commerce, the basis for sovereign control over commercial activity will be increasingly questioned.

Legal: The global nature of the Internet means that any service may be subject to several jurisdictions. This may lead to uncertainty as to which law applies to any contract or transaction. In addition, firms offering services via the Internet will need to consider any requirements imposed by the law of the consumer's country - including statutory consumer rights, data protection and so on.

There may also be instances where particular jurisdictions provide better support for Internet commerce than others. Countries may even compete for new business in this way. Certainly, firms offering services via the Internet are likely to weigh the effect of contract law, data protection requirements, insolvency law etc. before establishing themselves in any particular location. As far as payment and settlement systems are concerned, the applicable law will govern issues such as when a payment is final, up until what point a payment instruction may be revoked, whether there is a "zero hour" rule, etc.

Regulation: The Internet also presents new challenges for regulators. Existing laws may be flexible enough to allow some regulators to maintain jurisdiction over activities conducted via the Internet but new legislation may be required in other cases. Even where a regulator does assert jurisdiction, it may be difficult to take action against an offender if he is based in another country. In some cases, it may even be difficult to track down exactly where an offender is based.

Customers based in the UK can already conduct business with offshore banks and investment companies which advertise via the Internet. But developers of e-cash and payment schemes may not necessarily be banks; indeed they may be totally unregulated. This would raise issues of depositor protection and systemic risk. For instance, an Internet user in the UK can open a bank or brokerage account abroad from his PC. If an investor elects to buy bonds via a foreign virtual stockbroker and pays him from his account with a foreign virtual bank, no part of the transaction has occurred in the UK. UK regulators may feel, nonetheless, that they have a responsibility to protect the investor/depositor, even though it would require an assertion of extra-territorial jurisdiction. How regulators handle these issues will have a direct impact on...
The development of Internet commerce, and consequently on the progress of the payment and settlement systems which support it.

**Taxation:** This is a particularly interesting aspect of Internet commerce, and associated settlements. The ability of states to raise taxes on consumption will be challenged by Internet commerce. Mervyn King, chief economist at the Bank of England, has already raised the concern that a global, virtual economy with dematerialised goods and payments undermines old methods of taxation at a time when taxes are increasingly linked to consumption. At the present time, Customs & Excise may still be able to collect duty on US CDs ordered over the Internet as they are delivered by mail. But would it be so successful if the CD was downloaded directly?

Taxation of Internet commerce will also play a role in the choice of location for Internet business and on the specific systems used to support it. There are already precedents. For example, global telecom companies long avoided establishing a presence in the UK because of the imposition of VAT on sales, regardless of where customers are located or the services rendered. Internet businesses will likewise make choices about location and structures based on taxation regimes.

**Monetary policy:** Lastly, the development of Internet payment systems could influence the effectiveness of monetary policy.

Just as the inter-bank and institutional markets are already globalised and relatively free of regulatory constraint, the Internet has the potential to widen choice at individual and small business levels. Once money is denominated as electronic cash units, savers will be able to trade their savings via the Internet for a more attractive currency. Monetary authorities in countries with currency convertibility and e-cash systems may have little control over such transactions. Some commentators have warned of greater financial instability, particularly in weak currency states. Others counter that the need for monetary discipline will be reinforced by the market if consumers have more flexibility.

**7. Conclusion**

The form and speed of development of electronic payment systems will have a strong influence on the way that commerce evolves on the Internet. But though a tremendous amount of activity is going on in this area, it is too soon to say with certainty how the picture might look as little as five years hence.

Although banks – the traditional suppliers of payment and settlement services – have a head start in this area (insofar as plastic cards are currently the most convenient way to pay for purchases over the Internet), their position seems far from secure, for several reasons:

- One is that the banks themselves have not made an early bid to establish Internet-specific payment systems.

---

Another is that credit cards are not ideal: they are too expensive and are felt to be too insecure.

A third is that most of the initiatives so far have been made by non-banks who see a business opportunity, like Netscape, Microsoft and BT.

But while the field for suppliers remains wide open, it is increasingly clear what a successful Internet payment mechanism will have to look like: simple, secure and verifiable, and probably based on a non-accounted e-cash system.

It happens that banks possess many of the capabilities to deliver such a system: they have experience of payment mechanisms, and they have a reputation for security and confidentiality. The SET standard should reinforce the role of credit cards. But if e-cash comes out on top, banks like NatWest will have the experience of Mondex to guide them.

There may also be public policy reasons why it would be preferable for banks to supply Internet payment systems: it would keep monetary matters under closer control, and it would ensure that those systems were underpinned by regulated institutions. On the other hand, banks have to bear the burdens of heavy regulation and costly legacy systems, none of which hinder their non-bank competitors, and those self-same competitors are certain to challenge any official presumption that payments should be the preserve of the banks.

It seems very likely that, sooner or later, retail payments via the Internet will take off. However, the Internet as such may not have as bright a future for wholesale payments, where closed, high-security systems are more likely to predominate. Nevertheless, the Internet could have a role to play in back office administration and authorisation of trade.

The real question is to what extent banks will benefit from these developments, and to what extent they will find their franchise eroded. The group was unable to reach a consensus on that, but it is clear that the potential is considerable on both sides.
SECTION THREE: INTERNET DRIVERS

Chapter three: Security

Summary: Although existing levels of security on the Net are not as weak as many believe, security is a real problem because of the open nature of the Internet and the fact that many managers are unaware of how their computer networks can be accessed from the Net. That said, there are solutions — particularly for fairly specific applications. The most important is probably wider use of strong encryption — and that is becoming more realistic as the US eases export restrictions (which have traditionally been very tight). Encryption can produce an acceptable level of user and message authentication and non-repudiation, as well as confidentiality. In addition, the security of systems that are hooked up to the Internet can be much improved by use of firewalls and virus protection tools — many of which are now available commercially. Even more important, however, is the existence of consistent and regularly reviewed security policies. Internet security must be a management priority.

Chairman: Nick Collin            SRI International
Vice-chairman: Tom Parker        ICL
Rapporteur: Nick Collin

Working group members:

   Robert Barnes
   Pamela Clark
   Tommaso Corrado
   Richard Hackworth
   Tony Harris
   Philip Harrison
   John Howell
   Nigel Howell
   Liz Miles
   Carol O’Connor
   Steve Patten
   Mark Stirland

Office of the Comptroller of the
Currency, US Embassy
SBC Warburg
Guildhall Ltd.
Maple Network Consultancy
Morgan Stanley
Crime Methodology
Consultants
Mercury Communications
NatWest Bank
Vision in Practice
M&G Group

A representative from BACS also participated in the group.
1. Introduction
The explosive growth of the Internet has focused attention on the need — real and perceived — for greater information security. As communication by e-mail becomes commonplace and electronic commerce grows, there is an increasing concern that confidentiality and authentication (i.e., keeping transactions private, and ensuring that people really are who they say they are) could be compromised. This is a particular concern for financial institutions since the secure transmission of financial information is central to their operations, and any damage to their reputation for integrity and trust could be catastrophic. However, this chapter also makes it clear that banks could benefit as well: their reputation could be exploitable in a growing market for information security services.

The present chapter covers the findings and recommendations of a working group set up by the CSFI to address Internet security, and specifically the question: “What new security issues does the Internet raise for financial institutions?”

2. Is Internet security a problem for financial institutions?
Although there is widespread concern about Internet security, there are few reliable statistics on crime perpetrated over the Internet. However, there are enough frightening statistics to lend credence to the tales of gloom told by the security experts (who obviously have their own axes to grind). For instance:

- It has been estimated that there are about 20,000 actively malicious hackers in the US alone.

- The Defense Information Systems Agency (DISA) in Washington recently conducted a series of test attacks on military systems through the Internet. Two thirds of these were successful. However, only about one in 150 was ever reported.¹

Results of DISA vulnerability assessment

Financial institutions are particularly at risk:

- Many Net applications involve communicating sensitive financial information: e.g. home banking, securities dealing, and electronic shopping.

- Electronic commerce over the Internet involves new payment mechanisms. By 2000, it has been forecast that the annual value of trade on the Internet will reach US$600 bn; even if that is way too optimistic, huge sums will be involved.

- The finance industry is specially vulnerable to reputation risk. Because of this, the perception of insecurity is all-important, almost irrespective of whether this perception is valid.

On the other hand, secure communication over the Internet presents new business opportunities for financial institutions – though others will seize this if they do not.

3. Assessing the seriousness of the problem

It is very difficult to make a realistic assessment of the seriousness of the security threat posed by the Internet. On the one hand, it is claimed that the frequency of incidents is small, and that security experts who highlight the risk stand to gain most from it. On the other hand, institutions which have been subject to attack are reluctant to publicise the fact for fear of undermining their credibility. The working group takes the view that the potential risk (actual and reputational) is so great that all financial institutions need to take it very seriously indeed. The group is, moreover, directly aware of several disturbing attacks which occurred as this report was being prepared, including:

- a Scandinavian bank, which was infected by a virus sent via e-mail from its London branch; and

- a UK company which received a virus from one of the world’s largest database software companies.

There is also no doubt that general use of the Internet can compromise confidentiality. The Internet was not designed with confidentiality in mind: it is an open system in which every transmission that is not consciously made secure can be copied and analysed. Un-encrypted data on the Internet – and even intranets – is more easily accessible than the equivalent data in the mail or on the telephone.

Risk = Vulnerability x Threat: There are two dimensions of risk:

- vulnerability, i.e. how easy is it to violate security? and

- threat, i.e. what will it cost if security is violated?

By combining the two we arrive at a risk assessment, or expected security cost: notionally, the cost of a violation multiplied by the chance that a violation will occur.
On the Internet there is a mixture of vulnerabilities and threats, depending on the way the Internet is used:

- An organisation with an isolated Web site for general public access, i.e. to display its wares, has a reasonably well-understood vulnerability. The threat is relatively small; therefore so is the risk.

- The risk is increased if the Web site is connected to the company’s internal computer network, but it is still generally manageable. Similarly, a well defined application (such as home banking over the Internet) – provided it is well designed and well managed – can be engineered so that the threat is acceptably low.

- If, on the other hand, an organisation permits its staff many forms of access to the Internet – for example Internet mail, file transfer and indiscriminate access to World Wide Web sites – then vulnerability can be high and difficult to control. The threat can also be considerable, depending on the connectivity permitted. This can therefore be a high risk venture that needs strong security.

In all cases, the unstable nature of the security problem makes it difficult to ensure that the desired level of security has really been achieved. In part, this instability reflects the fact that the hacker community is growing in size and sophistication. In part, it is a result of the practical difficulties of trying to control Internet access and connectivity over a large organisation. As the entire security process is only as strong as its weakest link, even a single oversight can undermine the whole security mechanism. The “open architecture” of most company-wide computer systems does nothing to alleviate this problem.

This leads to an important distinction between:

- specific business applications, where the vulnerability can be controlled and the overall risk is therefore potentially knowable and manageable; and

- more general Internet access where threats and vulnerabilities are less well-understood and more difficult to control and where, therefore, the overall risk can be high and difficult to manage.

**Specific business risk can usually be managed:** If an organisation is running a specific business application over the Internet (anything from home shopping to large scale wholesale financial transactions), the *vulnerability* is normally fairly well bounded and the security measures needed are reasonably well understood; indeed in many areas they are standardised. However, the *threat* of financial fraud may well be high. A successful attack particularly on wholesale financial transfers could cost millions; so the measures taken need to be very strong. Conventional fraud risks are also higher because of the speed at which cash can be taken out of the system, and because of the relatively low risk to the perpetrator. Such crimes can be depressingly cost-effective.
Vulnerability is increased because the “window of opportunity” for the criminal is open 24 hours a day, seven days a week. Furthermore, the attacker, who may be thousands of miles away, can be in and out of the system very quickly.

On top of this, the vulnerability of commercial organisations is often higher than it need be because security technology is not properly understood by the organisation concerned and is inadequately managed.

Useful computer security "link" pages: Below is a selection of security link pages and information available on the Net. A stroll through them should convince even the most sceptical that the Internet does represent a step-level change in the size of the threat to IT systems:

| www.ex.ac.uk/-relaint/links.htm | www.cs.uml.edu/~kenny/sec.html |
| wwww.econ.com/action/links.htm | www.clw.edu/separable/compsecurity.htm |
| www.scafe.com/security.html | webk1.ku.ac.uk/~boubout/securtiy.html |
| www.apanet.com/tp/group/secc001.html | www.insect.soe.ac.uk/crypto/security.html |
| www.tufts.edu/~varela/library/security.html | www.engl.ucr.edu/~mac/crypto.html |
| caa.nccu.edu/~yokol/library/security.html | www.caio.ca/info/contents/secure.html |
| www.169.146.70.100/av-link.html | cooql.ciprint.univ.ac.at/~shin/secure/security.html |
| www.engadget.com/~mch/secdir.html | www.ncaeo.ncc.edu/~lucsec.html |
| psy.math.wlu.edu/~jilloff/security.html | www.simon.net/~links.html |
| www.users.dicoll.co.uk/~rego0600/nwlinks.html | eddie.cis.uoguelph.ca/~fouquet/links/security.html |
| loose.opolis.org.au/security.html | www.cet-nl.or.fr/WEB_LINKS/home.html |
| netlab.korea.ac.kr/research.html | cplim.wharton.upenn.edu/~shou/opem90.html |

But if the application is carefully designed and expert advice is followed, it is possible to manage both threat and vulnerability so that the overall risk is acceptable. This is partly because advanced cryptographic technology is now available to augment the security provided by more conventional “firewalls” and by proper internal procedures. But it is also because the risk in a specific application can be defined and controlled – even if it cannot be completely eliminated.

In this sense, conducting financial transactions over the Internet is subject to the same security concerns as any other inherently insecure medium, such as the telephone or the mail. Financial institutions have successfully operated in this insecure environment for years, even centuries – indeed, it is one of their
core competencies. What the Internet introduces is a new environment with which they need to become acquainted.

**General access via the Internet can pose a much greater risk:** A potentially more serious risk (because it is less easily managed) is the trend for organisations to use the Internet, or Internet technologies, to communicate more extensively internally and with the outside world. As corporate boundaries dissolve, the risk of malicious or accidental damage to information systems, or of unauthorised access to sensitive data, increases significantly. Like most organisations, financial institutions do not yet fully understand the risks inherent in this new way of operating.

For instance, it is increasingly common for staff to communicate with parties outside their organisations via e-mail over the Internet. More and more employees also routinely access the World Wide Web to download documents or software. Staff may access the Internet from the office or, with the growth of "telecommuting", from their homes or other insecure outside locations. Many organisations are also building "intranets" - using UNIX, TCP/IP and other "open" Internet technologies as the basis for their internal corporate networks - which, almost by definition, allow relatively seamless interconnection between the internal and external corporate environments, as well as easy access to internal corporate systems.

Organisations are adopting this approach because it produces greater efficiency at low cost. What is not so widely recognised is that it can also produce a dramatic increase in security risks, including:

- unauthorised access to confidential information, either by intercepting messages or by penetrating internal corporate systems;
- targeted or accidental damage to corporate systems by hackers; and
- targeted or non-targeted virus attacks.

Most organisations already conduct extensive cost-benefit analyses of the implementation of new technology, but they seldom carry out a "security audit", and even less frequently do they try to quantify risk in cost-benefit terms. In consequence, security does not get the priority it should, or is left to IT budgets, which means that IT departments get over-stretched.

In summary, general access to the Internet carries with it high vulnerability and high threat, and therefore the overall level of risk is high. Furthermore, because the threats and vulnerabilities are effectively unbounded (applying to all employees and all information systems within an organisation), they are much more difficult to control than specific business applications.
Viruses and the Internet: Although no specific virus threats are created by the Internet, it can be a source of viruses and, therefore, the weak link for organisations with a high dependence on networks, no matter how secure their systems. The damage caused by a virus may be very large because it can paralyse an organisation and be costly to eliminate. The more centralised an organisation's data storage, the greater the threat.

According to Computer Virus Cost Analysis, an August 1995 study by the US National Computer Security Association, the average company site (with 1,000 PCs) spends over US$300,000 on computer virus clean-up each year.

The vulnerable points are at the interface between internal networks and the Internet. Traffic is difficult to monitor, and viruses often 'hide'. Moreover, the traditional guardians of data (IT/MIS departments) are usually bypassed in Internet traffic, which increases the likelihood that a virus will pass undetected. There is also a threat from infected floppy discs which are brought into the building by employees or subcontractors.

Consider the following very plausible scenario:
An employee at a financial institution receives an e-mail over the Internet from a business associate. The message has an attachment: a Word document with a "macro" virus. The recipient opens the document and then makes it available on the company's server for others to see. From this point, the entire institution may soon become infected. If another employee now sends e-mails with similar attachments to other financial institutions, the seed of potentially global systemic corruption is sown.

A further threat may come from downloading software from the Web or invasion by software "agents". As part of the trend towards network computing, it is becoming increasingly common for Web sites to download automatically "applets" written in the Java computer language into the user's computer to execute a specific task (such as formatting associated data or calculating a result). Although it is claimed that Java applets and agents are effectively insulated from the receiving terminal's operating system - and although there have at yet been no reported case of a successful Java virus (the general belief is that viruses cannot be written in Java) - this is a rapidly developing technology and it seems prudent to regard the potential risks as high. Not long ago it was thought impossible to pass on a virus by means of a "macro".

The scale and intensity of Internet usage often make traditional protective measures ineffective against these sorts of risks. The organisation-wide impact of Internet use requires senior management to understand the implications and foster disciplined usage throughout their organisations, though a balance needs to be struck between risk control and over-restrictive network usage rules.

4. Solutions
There are really three main weapons available to the corporate user of the Internet to enhance the security of his operations:

- more extensive use of the fast-growing field of cryptography – the full potential of which is still evolving;

- greater use of "firewalls", "sheep dips", anti-virus programmes and other internal systems for automatically blocking intruders and for seeking out those who have nevertheless gained unauthorised access; and
tighter security procedures imposed on all staff (since the biggest vulnerability of all is negligence).

Cryptography: Cryptography can be the major technical solution to many of the security problems posed by specific financial business applications on the Internet because it is capable of providing both confidentiality and integrity. It is, therefore, worth dealing with in some detail. Basically, it comes in two flavours: symmetric and asymmetric, the latter often being referred to as public key cryptography.

**Cryptography made simple:** Cryptography is important in helping to ensure the security of information transmitted across networks. It is of particular importance in the commercial use of the Internet, where many problems need to be solved, including:
- customer authentication;
- server authentication;
- confidentiality of messages;
- non-repudiation of transactions; and
- proving the integrity of message content.

They can all be solved by using tools and products based on cryptographic techniques.

At the heart of any cryptographic product or solution is a secret that is used to exclude all those not entitled to read, create, or modify information. The strength or effectiveness of a cryptographic product is measured by the ease with which the "secret" can be discovered by unauthorised people.

In a cryptographic product or system, the secret will always be the key - and it may also be the algorithm.

A cryptographic algorithm is a mathematical transformation of a bit stream according to a complex set of rules. If the same transformation was used continuously, it would become easier to break. Also, an algorithm may need to be used by different groups of users. Designing a cryptographic algorithm is not cheap, and a developer will want to sell it to many different groups of users. Variation between implementations is, therefore, introduced by a cryptographic key. The key is a variable that significantly changes the transformation process. One can compare the cryptographic algorithm to a combination lock, and the cryptographic key to the combination used in the lock.

Some encryption algorithms are well known - DES (Data Encryption Standard), a popular algorithm, is a published standard. Others, such as Skipjack, are kept secret.

Cryptographic algorithms fall into one of two classes: symmetric, or private key, and asymmetric, or public key. Symmetric algorithms are so called because the same algorithm and key is used for both the encryption and decryption process. Asymmetric algorithms are so called because the key used to decrypt a message is different from the one used to encrypt it.

- **Symmetric (private key) algorithms:** A symmetric algorithm uses a secret key to encrypt a message to provide confidentiality and at the same time make it impossible to change or forge a message with any confidence that the results will be meaningful when the message is decrypted. The key is kept secret, hence the term "private key algorithm". The most widely used symmetric algorithm is DES. Symmetric cryptography is the fastest technique for encrypting and decrypting information, but it suffers from the need for a complex key management system. Each pair of users needs a secret key that must be generated, exchanged, stored and used in conditions of utmost
security. For an application like home banking, it may require a bank to hold 50,000 private keys, an onerous task. Fortunately there is an alternative.

- **Asymmetric (public key) algorithms:** Although at first seems impossible, there are techniques available that do not rely on secret keys to encrypt information. Each user has two keys: a public key, and a private key. The public key can be published in a directory (much like a telephone number). Anyone wanting to send a secure message to a particular individual can do so using his public key. Whilst information can be encrypted by anyone using the public key, it can only be decrypted by the person who knows the secret key - the person for whom the message is intended. This means that all anyone need protect is his own private key.

Public key cryptography is founded on an intractable mathematical problem. There is no easy way to factorise large numbers (500+ digits) whose only factors are two large prime numbers. The public key is the large number, and the private key is its two factors. The most widely used asymmetric algorithm is RSA (named after its inventors).

Public key cryptography requires a lot of computational power, so it is not normally used to encrypt large messages to provide confidentiality (symmetric cryptography is used to do that). It is, however, the most convenient method to transmit symmetric keys securely across an insecure network, and because it is easy to do, the symmetric keys can be changed with every message if need be.

Public key cryptography has other interesting properties. First, if you send someone a message encrypted with your private key, anyone can decrypt it, but anyone reading it can be certain that it came from you. No-one else could have encrypted it with meaningful results. In other words this is an elegant method of authentication. Secondly, it is possible to use a “digital signature” to guarantee both message integrity and non-repudiation. Banks have long used hashing techniques (like hash totals of account numbers in the old batch processing days). If a message is hashed, and the result encrypted using a private key, the message is proof against tampering, and has effectively been signed. The sender cannot deny generating the hash since no-one else had access to his private key. Of course, confidentiality can be added by further encrypting the message using symmetric cryptography, or encrypting it using the addressee’s public key.

**Cryptography and the law:** Strong cryptography is a double edged sword. While it makes commerce across the Internet possible, it also allows terrorists, drug dealers, and other undesirable people to communicate securely. Electronic monitoring of communications is a powerful weapon in the armoury of law enforcement agencies. They have always resisted the widespread use of strong cryptography (strong algorithms, and long keys). Some countries such as the US and UK put controls on the export of cryptographic products. Others such as France and Russia also control its import and use. Since many of the products used in banking are sourced from the US, this rule is most unpopular with both the vendors and the potential purchasers.

A recent proposal by the Clinton Administration will relax the rules. Provided that a trusted party (which may be the user) undertakes to make the encryption keys available to law enforcement officers armed with an appropriate court order, there will be few restrictions on export from the US of cryptographic algorithms - and the algorithms may use longer keys. This is known as a “key escrow” or “key recovery” arrangement.

**Symmetric cryptography** is typically used to ensure confidentiality and integrity for data sent over the Internet. Given a sufficiently strong cryptographic algorithm and properly generated keys of sufficient size, the level of protection provided
can be very high indeed. The Data Encryption Standard (DES) is the most well-established symmetric algorithm.

Asymmetric, or public key cryptography, is used to provide digital signatures which can authenticate users and messages, and also support the distribution of keys for use in symmetric cryptography. The most commonly used algorithm is called RSA (named after its inventors, Rivest, Shamir and Adelman), though Western governments would prefer DSA (Digital Signature Algorithm) to be used.\footnote{The reason is that RSA encryption can be used to encrypt data as well as to sign it. This encryption can be very strong, making the encrypted document impossible to decipher even for government agencies. As a result, it is illegal to export certain types of RSA technology from the US. DSA cannot encrypt (it is only a signature algorithm) and therefore does not lock governments out.} The problem for non-US users is that these algorithms are covered by US patents which still have several years to run, and are tightly controlled by US export restrictions, though this may change (see below).

Standard application-level protocols that include cryptography are now emerging for the financial community. These have the advantage of being able to define how the encryption methods are used, alone or in combination with others — to ensure the overall security of an application. The most likely standard to dominate in the evolutionary world of the Internet is the SET (Secure Electronic Transactions) specification supported by Microsoft, Netscape, Visa and Mastercard. (Further information on SET can be found at http://www.rsa.com/set/)

Intermediate between the encryption standards and application level protocols are other security standards, of which the most important currently is probably SSL (Secure Sockets Layer) which defines network level security arrangements between server and client, and which is built into all copies of Netscape’s Navigator browser.

Export restrictions on cryptographic technology: Most developed country governments restrict the export of "strong" cryptographic technology to prevent it being exploited by criminals or hostile powers. In the US, which owns the patents to the strongest algorithms, strong cryptography is classified in the US Munitions List as an export-controlled commodity, and is also subject to the International Traffic in Arms Regulations (ITAR). As a result, software incorporating strong encryption can be sold in the US, but can only be exported with difficulty, though President Clinton recently pledged to ease some of these restrictions by permitting export of 56-bit encryption technology. In addition, the OECD is now getting in on the act — publishing non-binding guidelines on the growing use of cryptography in electronic commerce. The key point is the attempt to establish the principles by which law enforcement agencies around the world can get access to encrypted data.
Cryptanalysis and attacks on cryptosystems: Cryptanalysis is the art of deciphering encrypted communications without knowing the proper keys. There are many cryptanalytic techniques, including:

- **Ciphertext-only attack**: This is where the attacker does not know anything about the contents of the message and must work from ciphertext only. In practice, it is not impossible to make guesses about the plaintext, as many messages have fixed format headers. Even ordinary letters and documents begin in a predictable way. It may also be possible to guess that some ciphertext blocks contain a word.

- **Known-plaintext attack**: The attacker knows or can guess the plaintext (i.e. original data) from some parts of the ciphertext. The task is to decrypt the rest of the ciphertext blocks. This may be done by determining the key used to encrypt the data, or via some shortcut.

- **Chosen-plaintext attack**: The attacker is able to have any text he likes encrypted with the unknown key. The task is then to determine the key used for encryption. Some encryption methods, particularly RSA, are extremely vulnerable to chosen plaintext attacks. When such algorithms are used, extreme care must be taken to design the entire system so that an attacker can never choose encrypted plaintext.

- **Man-in-the-middle attack**: This attack is relevant for cryptographic communication and key exchange protocols. The idea is that when two parties are exchanging keys for secure communications, an adversary puts himself between the parties on the communication line. He then performs a separate key exchange with each party. The parties will end up using a different key, each of which is known to the adversary. The adversary will then decrypt any communications with the proper key, and encrypt them with the other key for sending to the other party. The parties will think that they are communicating securely between themselves, but in fact the adversary is hearing everything.

- **Timing attack**: This new form of attack is based on repeatedly measuring the exact execution times of modular exponential operations. By measuring how long it takes to encrypt/decrypt a given message, a lot can be inferred about the key(s) being used. It is relevant to RSA, Diffie-Hellman, and Elliptic Curve methods.

US software companies designing products for export have had to produce special versions which incorporate only relatively weak encryption. This means that, until now, many non-US companies have been restricted to 40 bit keys which can be cracked by determined hackers. Financial institutions are normally granted exemptions from US export restrictions for applications which are of a genuinely financial nature. Thus it is possible to use strong symmetric algorithms for limited encryption of well-defined sensitive data such as passwords, or PINs. For example, strong symmetric DES encryption is routinely used by UK banks to protect ATM transactions. Use of this stronger encryption level (128-bit) with Internet transactions would make the Internet safer than settlement systems (such as SWIFT) currently in wide use in the financial service sector.1

1. Several financial institutions operating in London have obtained exemption from the US restrictions by demonstrating that their use of such technology is in line with their regular business and does not represent a security risk to the US government. Others have been forced to register as arms dealers for US purposes, so that they can qualify for export licences on strong encryption.
In addition, there is normally no serious difficulty for financial institutions to use strong asymmetric technology, such as RSA or DSA, for purposes such as authentication, non-repudiation and key distribution which do not, of themselves, render messages unreadable — and which do not, therefore, pose a threat to the authorities. Institutions are also fairly free to use strong encryption within country borders, where no export of the technology is required. In this context, it is worth noting that Germany’s Siemens Nixdorf has just started to promote a new product, TrustWeb, which incorporates 128-bit technology developed in Ireland (TrustWeb: http://www.trustweb.com).

Export control of cryptographic systems: The export of commercial information security goods, both hardware and software, is subject to tight controls. In the past, NATO countries based their controls on CoCom, but this is being replaced by the so-called “Wassenaar Agreement” reached by the “New Forum” (CoCom’s replacement). Certain countries, such as France and Russia, have additional controls.

Within the EU, exports are governed by the Dual-Use and Related Goods (Export Control) Regulations. Under these, an Open General Export Licence (OGEL(x)) is needed to export goods which provide access control and/or authentication, or which are specially designed for banking transactions.

In the US, two government agencies control the export of cryptographic products: the Bureau of Export Administration in the Department of Commerce, and the Office of Defense Trade Controls in the State Department. State licelses with the National Security Agency (NSA) in deciding, on a product-by-product basis, whether to permit export. If approval is obtained, further exports are controlled by the Commerce Department, which has less stringent requirements.

Since 1992, France has implemented tough controls over cryptography within its territories. Two regimes govern products implementing authentication and confidentiality: the regime of preliminary declaration covers the former and the regime of preliminary authorisation the latter. In the future, it is expected that the regime of preliminary authorisation will evolve towards simplified rules, based on the use of key escrow techniques.

In 1997, French legislation will set up a regime of free cryptography use, providing that users rely upon TTPs (in this context, a euphemism for key escrow).

The situation in Japan is different since the legal system limits the possibility of applying key escrow techniques. Moreover, Article 21 of the Constitution lays down the right to secrecy of communication. Japanese courts are therefore extremely cautious about approving wire-taps for criminal investigations. Furthermore, the Japanese government supports the widespread use of cryptography in order to encourage the development of a Global Information Infrastructure.

The problem comes when institutions wish to use encryption to maintain the confidentiality of large volumes of information (such as e-mails, research reports, or tender documents). If they feel that the 40-bit encryption, which is standard in many software packages, is inadequate, they must either build applications in-house using proprietary encryption technology (which is expensive and non-standard), or obtain a locally supplied product. This constraint has been a factor hampering the growth of the Internet.
In the future, it is likely that another solution will emerge in the form of "key escrow" arrangements, whereby standard, commercial, strong encryption technology can be used – provided the keys to read the encrypted information can be recovered by the authorities if required. Key recovery, or at least the promise of it, will be a condition of the export of 56-bit encryption which the Clinton Administration has promised.

What this all amounts to is that although they are frustrating and bureaucratic, export restrictions are unlikely, in practice, to be an insuperable barrier to financial institutions wishing to secure a genuine financial application, unless this involves transmitting large volumes of unspecified encrypted information such as e-mails.

Financial transactions over the Internet can be secure: Cryptography provides a basis on which to build secure applications using more or less conventional security tools and techniques which are well-known to financial institutions.

For most applications, the main requirements are for user authentication (proving someone is who he claims to be), message authentication (proving that a message has not been changed in any way) and non-repudiation (proving that someone sent a message even when he denies it). These can all be achieved by available public key cryptography.

There may also be a requirement for confidentiality. This applies to high value transactions (such as wholesale security trading), but it can also apply to those retail applications where there is a requirement to transmit sensitive information such as a PIN or a credit card number.

Beyond this, additional steps need to be taken depending on the particular threat/vulnerability profile of the application. For example, most retail applications need some form of strong authentication to tie a particular individual to a transaction (strictly speaking, SET only verifies the client software, rather than the owner of that software). The simplest measure is to use private passwords or PINs, but this may imply the need for encryption to preserve their confidentiality. A stronger measure is to use calculator-like devices to generate one-time passwords which are different for each transaction. In the future, it seems likely that smart cards, or perhaps even voice imprinting, will be used.

Another area which must be addressed is that of certifying users of a financial service, and arranging for cryptographic keys to be distributed and maintained in a secure manner. Various more or less standard schemes have been developed to handle this problem. Although complex, they are now well understood by most financial institutions and a high degree of overall security is therefore possible.
Although, in general, financial transactions can be conducted over the Internet with a high degree of security, two other factors need to be addressed before they become widely accepted:

- First, the publicly perceived level of security is very low. A study conducted by the Georgia Tech Research Corporation found that 60% of respondents cite security concerns as the primary reason for not buying merchandise through Web sites.

- Second, a wide range of alternative payment/certification schemes is currently available which is confusing to the public and tends to undermine the Internet as a payments medium.

**A commercial certification scheme:** VeriSign, created in 1995 as a spin-off from RSA Data Security, is a leading issuer of digital IDs for the Net, and is trying to convince users that digital certificate schemes are a solution to the security problems holding up wider Internet commerce. VeriSign issues class 1, 2, and 3 certificates that authenticate the identity of parties in an electronic transaction at varying levels of security.

Essentially, the system runs on the basis of electronic "keys", programmed by VeriSign. Contained on these keys is information about the user, protected by a complex system of cryptographic shields that the company guarantees.

When a transaction occurs, the company extracts the relevant information from both parties and undertakes the exchange in a neutral, third-party setting, before sending confirmation back to both customer and supplier. By maintaining this separate exchange, the company ensures neither party involved has an advantage over the other.

However, VeriSign is not the only certification authority. GTE has announced a CyberTrust certificate authority service, and the US Postal Service is running a beta test of its own. IBM also intends to enter the arena, and the EU is trying to promote various European initiatives. So far, however, no major financial institution has attempted to become a certifying authority in its own right.

More information can be found at http://www.verisign.com

It would seem that there is a clear case for co-ordinated action on the part of the financial community, to:

- standardise methods for securing transactions;

- publicise those standards and educate the public into accepting them; and

- lobby the US government and other authorities for further easing of restrictions on the export of strong cryptographic technology, particularly with regard to key escrow arrangements.

**Other forms of security:** Uncontrolled or casual use of the Internet and intranets for general communication and information gathering is dangerous for financial institutions. There is no single, simple solution to these problems. But an acceptable degree of protection is possible through the intelligent combination of cryptography, plus:
The Internet and Financial Services

- firewalls;
- virus protection tools; and
- appropriate security policies and procedures.

Firewalls constitute the main line of defence against unauthorised access and, to some extent, virus attacks. The principle is simply one of isolating internal systems, according to their degree of sensitivity, into zones separated by strictly policed barriers. This can ensure that if an organisation is penetrated, at least the inner core of mission-critical systems and data is protected. However, the firewall configuration has to be very carefully designed and managed, which requires a high degree of expertise and maintenance. And of course the internal servers must themselves be secured, using traditional information security tools. It should also be understood that firewalls normally work against incoming attacks. They are, therefore, usually less effective against so-called “Trojan horses” – programmes that could be introduced with the aim of “exporting” information (perhaps overnight) from one system to another.

Watching for viruses

Commercially available virus protection tools (such as Virex or Dr Solomon) can be used to scan incoming files for the presence of viruses; These tools are not foolproof and cannot detect newly-developed viruses, but they are an essential part of the armoury against attack and should be installed routinely on all PCs. Unfortunately, they offer only partial defence against the scenario of macro viruses in e-mail attachments referred to earlier, since it would be simply impractical to arrange for a firewall or router to scan every incoming message in real time. There is no easy answer to this problem. An extreme measure would be to forbid staff to receive external e-mails. Alternatively (as at least one major London bank is known to require), all incoming e-mails could be processed and scanned off-line through a single “sheep dip” before being forwarded to recipients. As a minimum, all employees should be instructed to scan all attachments and files downloaded from the Web before opening them. And, preferably, all incoming files should be processed on a stand-alone machine so that any infection cannot spread to other systems.

One intriguing possibility is that third parties (such as Internet Service Providers) could offer a useful service by scanning all incoming e-mail messages for viruses. It is even possible that financial institutions could provide this service as a new line of business.

Security policies and procedures are also essential. To be effective, technologies such as cryptography and firewalls must be applied within a comprehensive
security framework of the kind with which most financial institutions are already familiar.

At the top must be broadly defined security policies applicable to each main area of business. Simply stated, a security policy mandates the appropriate level of investment for the risks involved, and how that investment is to be applied. There is then a clear and complete mapping down to the lowest level of operations and systems with:

- detailed documentation of what technologies are to be used;
- definitions of what manual procedures need to be in place;
- identification of who is responsible for ensuring that security is maintained;
- clear explanations of what is to be done in the event of a breach of security; and
- broad agreement on how security arrangements are to be audited.

In this way, an institution can have reasonable confidence that nothing can slip between the gaps.

Every financial institution should update its security policies and procedures to ensure that the special risks associated with the Internet are taken into account. An effort should also be made to keep abreast of developments in new security techniques, as well as new threats.

One alternative, which has been suggested, is to arrange insurance to cover breaches of security — accepting that some loss is inevitable. The working group’s view is that this should be adopted only as a complementary measure to cover the residual risk after other measures have been put in place. Indeed, financial institutions might themselves offer insurance against security losses, given their expertise in risk management and superior knowledge of security issues.

Confidentiality as a problem: The obvious long-term solution to the issue of confidentiality is strong encryption of all sensitive messages using commercially available products, assuming that the US proceeds with its promised easing of export controls. Alternatively, or in addition, we may see the emergence of private versions of the Internet for closed user groups which — because they are not accessible to the general public and are relatively secure in a physical sense — offer some degree of protection. For example, The Bankers Network (now owned by Telelrate) has recently been established specifically to support private Internet protocol networking between authorised banks.

5. Summary of risks and measures to address them
The following matrix summarises our analysis of security risks and recommended solutions. The columns show the main risks associated with the Internet:
The Internet and Financial Services

- **Authentication failure**: The risk of fraud by unauthorised personnel posing as genuine users, tampering with messages, or repudiating previous instructions.

- **Targeted damage**: The risk of malicious attack on an institution’s systems or data by hackers and other hostile parties.

- **Non-targeted damage**: The risk of “accidental” damage, particularly as a result of virus infection.

- **Access to confidential information**: This can be either through message interception or unauthorised access to internal systems.

The top half of the matrix shows the level of risk (high, medium or low) associated with these categories in the two broad contexts of:

- specific financial transactions over the Internet; and
- general, non-specific use of the Internet for e-mail or Web access.

The bottom half shows the main counter-measures which need to be employed to combat each category of risk, with an indication of their relevance (high; medium; low).

<table>
<thead>
<tr>
<th>Risk Application</th>
<th>Authentication failure</th>
<th>Targeted damage</th>
<th>Non-targeted virus damage</th>
<th>Access to confidential information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific application</td>
<td>med</td>
<td>low</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>General Internet use</td>
<td>low</td>
<td>med</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>Counter measure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptography</td>
<td>high</td>
<td>high</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>Firewalls</td>
<td>high</td>
<td>med</td>
<td>med</td>
<td>med</td>
</tr>
<tr>
<td>Application level controls</td>
<td>high</td>
<td>med</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policies, procedures &amp; education</td>
<td>med</td>
<td>med</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td>high (anti-virus software)</td>
<td></td>
</tr>
</tbody>
</table>

6. Business opportunities for financial institutions

Internet security is a challenge for financial institutions — but it is also a business opportunity. There is clearly a huge demand for better information security among all users of the Internet, and this translates into a rapidly growing market for security products and services. Financial institutions could become leading suppliers to this market by virtue of their unique advantages, particularly:

- their image of trust, security and integrity; and
- their experience of security procedures and technologies.

There is already a multi-billion dollar market for hardware and software products (firewalls, cryptographic software and virus protection tools) dominated by IT suppliers such as Cisco, RSA and Netscape. It is not suggested that financial
Is my network computer system vulnerable to crime?: These questions are designed to help identify potential vulnerabilities. They form a basic checklist of weaknesses often encountered when tackling computer security.

Permitted access:
- Are authorised users trustworthy? (Those with the greatest privileges have the greatest chance for misuse. Don’t forget maintainers or developers.)
- Are responsibilities clearly assigned and operating procedures in place? (Do you have an up-to-date list of users for all systems, with their access level?)
- Are there adequate access and authentication procedures (e.g. password control for logging-on and access to applications, administration and system operating software)?
- Are there audit trails, and are checks undertaken to verify proper use?

Casual access:
- Can unauthorised persons gain access (e.g. are cleaners or visitors supervised)?
- Are passwords difficult to guess (and are they kept safe)?
- Can screens or printers be overseen (e.g. a screen next to a window)?
- Are storage media, inputs and outputs safely stored and disposed of when finished with? (Input documentation is often overlooked.)
- Is it necessary to restrict access to the computer area or to particular equipment?

External access:
- Is there a remote threat?
- Are there dial-in connections (i.e. can the system be hacked by telephone)?
- Is it clear which systems are linked together?
- Who has control over the linked systems?
- Do all linked systems have the same level of security? (Is there a weak link?)
- For the highest risk system, is there a threat from interception of electromagnetic transmission? (It is possible to tune-in to the weak radio signals that most computer equipment emits.)
- What is the value of gaining unauthorised access to the systems?
- What is the effect on business if systems are disrupted?
- Is what the system does clear? (What standard is the software written to? Have significant defaults - such as default passwords - been changed? Is there general access to dangerous commands - e.g. shut down, purge, delete? What happens in the year 2000? Is development and change to the system controlled?)
- Is there a contingency plan? (Are otherwise good procedures compromised at the time of a system breakdown, power loss, system testing, or when key staff are away? What about fire-drills?)
- What is current best practice?
  In establishing an organisation’s vulnerability, those from the chairman down must satisfy themselves fully with regard to the following:
  - Does my area of responsibility have a clear and well-researched policy on using the Net and on preventing crime via the Net?
  - Does it accept and abide by the policy that has been set out?
  - Is the policy efficiently and effectively enforced and updated?
  - Are breaches in policy dealt with in accordance with the danger to the organisation they represent?
The Internet and Financial Services

Individuals who cannot answer these questions may be unaware of the risks they run – and of the protection available.

**Response planning and implementation**: To be in a position to answer the key questions, Net users should consider setting up groups which would:

- form part of an organisation’s overall IT security team;
- include members of front, middle and back offices;
- seek outside help in areas where they lack expertise;
- co-operate with others at risk to provide mutual support (this is especially true for small companies);
- establish contacts on an industry or international basis to share experiences and information (larger companies);
- liaise closely with the authorities;
- develop and assess policies and commercial products for their cost-benefit, acceptability and enforceability/usability;
- work closely with users on implementation;
- establish regular monitoring and evaluation against pre-defined benchmarks; and

institutions compete in these markets, but there are a number of emerging areas where their advantages could be leveraged to great effect, especially:

- secure message transmission (including payments and EDI); and
- key management and certification (as Trusted Third Parties).

Secure message transmission is a natural extension of the banking industry’s existing effective monopoly over payment systems. The fact that the necessary infrastructure is already in place gives the financial community an important head start. Similarly, large financial institutions are particularly well placed to act as TTPs, to certify users, issue cryptographic keys, and manage large international networks of subscribers. However, the financial community will need to move fast since non-financial institutions are increasingly active in these areas. For example, organisations such as VeriSign, in which RSA has a stake, has already established itself as a TTP, while companies such as Microsoft, Netscape and Intuit are effectively offering secure message transmission – and are coming close to entering the payment systems market. The CSFI first began suggesting these new possible businesses for banks in early 1995.1

Financial institutions could, if they wished, create profitable businesses based on providing many other security products and services, such as keeping data confidential or even insuring against breaches of security. Some might argue that such services are too remote from their core activities. The counter argument is that maintaining the security of customers’ assets is a core financial services activity, and information is simply another asset. Other working groups have stressed that the Internet threatens to “disintermediate” financial institutions

1. Banks as providers of information security services, Nick Colkin, CSFI, 1995

A role for banks

174
from traditional strongholds. Providing information security services could be an important opportunity to redress the balance.

7. Conclusions and recommendations

The Internet does indeed imply a number of new security issues for financial institutions, some of them not intuitively obvious.

There is a widely held view, certainly amongst the public, that the Internet is an inherently insecure medium for payments and other financial transactions. This view is almost certainly false. Because these applications are well bounded and can be closely controlled, it is possible to use cryptographic technologies together with conventional security policies and procedures to ensure high levels of security.

On the other hand, general access by employees to Internet facilities such as e-mail and the Web constitutes a serious threat which is perhaps less widely appreciated. The risk to financial institutions of damage to internal systems or access to confidential information is exacerbated by their sensitivity to the adverse publicity which would almost certainly accompany such an incident. The risks can be mitigated by a combination of firewalls, data encryption, virus protection tools, and above all significant management effort devoted to culture change, awareness and training in appropriate security policies and procedures.

The other side of the security coin is that there are attractive business opportunities for financial institutions to provide security services to Internet users, such as certification, key management, and secure message transmission. The financial community is well placed to play a major part in this rapidly growing market by virtue of its reputation for trust and integrity, its experience of security tools and techniques, and its access to the technology.

It is surely in the interests of the financial industry as a whole to collaborate in researching best practice with regard to Internet security, promulgating standards, and lobbying governments for fewer restrictions on the use of strong encryption technologies. Meanwhile, each individual institution needs to examine carefully how its existing information security framework is impacted by the Internet, paying particular attention to measures for controlling general use of Internet facilities by staff.
SECTION THREE: INTERNET DRIVERS

Chapter four: Crime

Summary: Most internet crimes are really old crimes in new bottles – but that does not alter the fact that Net crime presents new challenges. The first is that no one knows how much is going on, which breeds all sorts of myths. Nevertheless, there is a lot of evidence that plenty of illegal activity is taking place. Of particular relevance to the financial sector is fraud (which already comes in many forms), software piracy, systems contamination and money laundering etc. It is worth remembering that financial organisations stand to lose in different ways – as direct victims, as unwitting hosts for illegal activity and as institutions whose strength is their reputation. The classic perpetrator of Internet crime is the “hacker” (whose motives may be fairly innocuous) – but there are strong indications that organised crime is not far behind. Unfortunately, the increasing sophistication of available technology now means that virtually anyone can attack virtually any system from virtually anywhere in the world.

Chairman: John Austin
Computer Crime Unit, Scotland Yard (until August 1996)
Vice-chairman: Andy Tester
Rapporteur: John Howell
Crime Methodology Consultants

Working group members:

Helen Addison
HSBC Holdings
Tommaso Corrado
Guildhall Ltd
Francis De Zulueta
Minet Group
Carol O’Connor
Vision in Practice
Jon Vagg
Loughborough University
Conor Ward
Lovell White Durrant
Andrew Wood
BBC World Service
Karl Ziegler
Centre for Accountability and Debt Relief

Martin Hollobone and Les Snelling, of the SIB, participated as observers in this group.

The group included other members who have requested that their names not be used.
1. Introduction

Background: The financial services sector has been quick to evaluate the Internet’s potential as a business medium. But new forms of business now host their own forms of crime. The Internet is already the object of a good deal of criminal interest, ranging from copyright violation, fraud and pornography to money laundering, information warfare and terrorism. The issue for Internet users is how serious a threat this poses, and how it can be countered.

This chapter offers an overview of these issues. The major considerations have been:

- to give some perspective to common fears and myths about the extent of crime on the Net;
- to assist bona fide providers, users and regulators by heightening awareness of the kinds of crime that occur on the Net; and
- to suggest how individual companies might assess and address their own vulnerability.

The group has been at pains to avoid being sensationalist. Crime on the Net is already shrouded in myth, and it would be easy to write a piece deliberately designed to scare the pants off any potential Internet user. Equally, it would be easy to be utterly po-faced. We have tried to strike a balance, eschewing rumour and the more sensational tales, but giving a flavour of what is (and is thought by responsible people to be) going on.

Definitions: To facilitate analysis of Net crime the group made the following distinction:

- The Internet is taken to mean one or more computers whose files may be accessed, or processes controlled, by another computer via an open communications system operated by a third party. Such a system is inherently vulnerable because it can be entered through any “window” that is left open, whether by design or accident. Its advantage is that it is open to the world, so that users (e.g. potential clients) can browse information.

- An intranet means computers whose files may be reached or processes controlled by another computer via a closed system under the control of the two communicating parties. Such systems are inherently more secure than Internet systems – provided that they are indeed “closed”. An intranet’s advantage is that it allows groups of users to share information or conduct transactions with each other, without the network being publicly accessible.

The group also defined two types of Net use:

- Transactions and settlements (e.g. execution of contracts/payments): The specific risk here is of fraudulent transactions and settlements.

- Information exchange (e.g. advertising): The specific risk is of interference with information.
Both for transactions and information exchange, the risk of crime is substantially higher on the Internet than on a more secure intranet. However, an intranet is, by definition, accessible by only a limited group – and that may not suit a user’s business plan.

One other point: on top of the direct costs of Internet crime, there is the risk that criminal activity will undermine confidence in the Net as a business medium or require counter-measures, whereby the costs outweigh the benefits of doing business on the Net.

2. Problem definition
Ignorance of what the Net is and does is a prime factor facilitating crime on the Net. For instance, the distinction between the Internet and intranets is generally not well understood. Many users are insufficently aware of the security implications of using a system with Net features, or of the risks inherent in their actions. There is also confusion as to the roles and responsibilities of the parties to Internet commerce: issuers, service providers and end users.

As a result people who have no need to be on the Net may be given e-mail addresses and default passwords which could render their systems vulnerable. Conversely, those who are knowingly connected may not be properly protected. These errors and misunderstandings can be exploited by criminals.

Types of crime: Publicly available information about crime on the Net is still scarce, and what little exists is soon enriched by fairy tales, not least on Net pages themselves. Moreover, the speed with which the Internet is expanding and the reluctance of victims to report security breaches mean that most data should be treated with suspicion. Nevertheless, there are several reputable studies which purport to give a picture of Internet crime, including annual studies by the Computer Security Institute (CSI) in San Francisco using survey questions worked out with the FBI.\footnote{Information on this and other studies can be found at the Computer Security Institute’s Web site at http://www.gocsi.com} In 1996, the CSI concluded that virtually all 428 responding organisations considered that their information systems were “under siege” – not least by remote dial-in services and Internet connections.

The CSI’s 1997 study has just been published. It focuses on the cost of computer crime. In particular:

- 75% of the 563 respondents reported financial losses from computer crime;
- of these, 16% cited losses due to unauthorised access by insiders, 14% due to theft of proprietary information and 12% due to financial fraud; and
- financial fraud alone is thought to have cost respondents over US$25 million, while the theft of proprietary information cost US$21 million.

Overall, the survey showed that the percentage of organisations that had actually experienced some sort of intrusion had risen from 42% to 49% last year, and that 47% now cited their Internet connections as a frequent point of attack.
So there is a problem. But is it a new problem or an old one in a different guise? One of the first points which the group agreed is that most forms of Internet crime are really modifications of more general types of computer crime – which in turn often have close parallels in the “real” world. Nevertheless, the group also agreed that connectivity can greatly increase the risk of crime – old or new.

From its own experience, the group identified the following forms of detected (or strongly suspected) crime as being facilitated by the growth of the Internet.

**Subversion of public infrastructure:** i.e. attempts – motivated by greed, ideology or simple bloody-mindedness – to cause mayhem by disrupting military and civil information systems, such as emergency service switchboards and area code level telephone exchanges. This is of special concern in the US.

This type of crime blurs into straightforward “hacking”, but some of its results are spectacular. They are also well-documented, mainly thanks to a May 1996 report by the US General Accounting Office on a series of attacks against the Department of Defense’s computer systems.\(^1\) The GAO report, plus the transcript of related testimony to the Senate Permanent Committee on Investigations, gives an astonishing insight into what can go wrong.

The incident was as follows. In March and April 1994, the computer systems of the US Air Force’s command and control centre (based in Rome, NY) were penetrated and briefly taken over by a computer hacker going by the name of *Datostream*. From Rome NY, *Datostream* was able to access systems at NASA’s Jet Propulsion Lab and the Goddard Space Flight Centre. He was also able to access Korea’s Atomic Research Institute system and very nearly provoked a serious diplomatic incident between North and South. Among the information that he obtained was the Air Force’s order of battle. All of this, so US authorities claim, was done by a 16 year-old British boy, using a 25 MHz 486 SX desktop with a 170 MB hard drive.

The boy’s intentions may well have been fairly harmless (he has pleaded guilty to several lesser charges relating to this incident), but the US authorities were concerned that innocent hackers could be controlled by others with more malign motives. As the Director of the CIA told the Senate hearings: “we have evidence that a number of countries around the world are developing the doctrine, strategies and tools to conduct information attacks I am convinced that the organised information warfare threat from both state and non-state actions will grow over the next decade as the technology proliferates”. Attention, therefore, focused on *Kuji*, another (albeit more mysterious) hacker who had apparently tutored *Datostream*, but whose identity was harder to crack. It now transpires that *Kuji* may well have been another underage British hacker with no motive beyond hacking. Nevertheless, the Rome episode was clearly one that shook the DoD to its core: never for a moment did the US government believe that its sensitive parts were so vulnerable.

---

The Internet and Financial Services

Sex-related offences: Surveys of Internet traffic show that a very high proportion relates to pornography. Most of this is soft-core, and not a real problem. However the availability of paedophile material and use of the Net to support the activities of potentially murderous paedophile groups is a major concern. The danger is that the Internet could be used to mask the identity of paedophile gangs, “snuff” groups etc., and that the ability to place pornography on the Internet creates opportunities for blackmail.

That paedophile groups use the Net is not really in doubt. One of the major search engines produces over 700 hits for the keyword “paedophile”. Most of these are for pages dealing with arrests, prosecutions and police co-operation. Nevertheless, it is still perceived to be a problem. In early 1996, French police arrested staff from two ISPs for allegedly tolerating paedophile “chat rooms” that they might reasonably have known would contain illegal material. Other ISPs in France subsequently staged a brief strike. Similarly, in December 1996, Bavarian prosecutors served Compuserve with a warrant to ban 200 allegedly pornographic news groups. UK authorities have also warned ISPs that they may be breaking the law if they do not block illegal material, and the UK Internet Service Providers Association (ISPA) is trying to set voluntary standards in association with the Home Office and the DTI. In August 1996, the Norwegian branch of Save the Children established a “cyercop” to search out child pornography on the Net. On the other hand, the US Supreme Court agreed at the end of 1996 to decide whether Congress had violated free speech rights by attempting to restrict indecency on the Internet.

The opportunities for blackmail that this creates cannot be ignored. Some members of our group felt that it was possible for a criminal to insert pornographic material into a person’s file, and then threaten that individual with exposure. (The mere possession of certain types of pornographic material is a crime in the UK.)

Fraud: This is a broad category, and one of particular interest to financial services providers, for obvious reasons.

The most notorious, though perhaps extreme, example is the Citicorp affair when several million dollars were re-routed from client accounts, allegedly by a Russian hacker.

More common are incidents involving:

• Pyramid schemes: In May 1996, the FTC shut down a Web site operated by Fortuna Alliance which, it claimed, had taken US$9m from investors in a pyramid scheme.¹ Although the allegations were denied by Fortuna, it has agreed to provide full refunds.

¹.  Euromoney, October 1996, p85.
• **Sale of non-existent “prime bank” securities:** This is an extension of a common “real world” scam that has grown greatly in recent years and lends itself to broadcasting over the Net.

• **Market manipulation:** There is evidence that certain small-cap stocks in the US have been aggressively (and perhaps illegally) promoted through ostensibly unconnected investor chat rooms (which boost stocks by word-of-mouth). In June 1996, the *Los Angeles Times* flagged a stock whose market value had risen from US$36m to over $1bn in three days – before the SEC filed a lawsuit. The stock fell by 80% before trading was halted.

• **Deposit solicitation:** This is a tricky area since there is nothing inherently wrong in the cross-border solicitation of deposits provided that investors understand what they are getting into. However, the Bank of England is concerned about foreign deposit-taking institutions advertising on the Net, touting above-market interest rates and tax advantages.

• **Credit card fraud:** The *Financial Times* reported in January 1997 that AOL had cut off computer users in Russia after fraudsters there used stolen credit card numbers to enter its network (and the Internet) without paying. There is a thriving underground market in Moscow in valid credit card numbers, and Internet access is just one of the uses to which they are put.

• **High return investments:** Offers of unrealistically high investment returns frequently appear on the Net, seeking to suck in unsophisticated (or desperate) investors.

On top of this, there are many examples of over-the-top advertising claims, particularly for work-at-home schemes, easy ways to make money, and “pump and dump” promotions.

**Hacking:** Defined as the unauthorised penetration of systems to copy, damage or otherwise access confidential information, this once (allegedly) harmless pastime is now a serious cause of malicious damage, thanks to the increased availability of computers and the low cost of access. The mere fact that a system has been penetrated undermines confidence in its integrity and the data it contains. Even if no damage has been caused (and much is done inadvertently), the system operator will still have to check this out.

The working group was most concerned about cases where hackers penetrate systems, leave so-called “flags” or “calling cards” and then present the owners with demands for money, backed by threats to destroy files if they do not pay. There is little doubt that incidents of this kind have occurred. What is less certain (despite a sensationalist *Insight* investigation by the *Sunday Times* in June 1996) is that anyone has actually paid up, or (as Internet lore would have it) has bought off the hackers by actually employing them.

**Software piracy:** The Net provides a low-cost, international distribution network for illegally copied software. The Business Software Alliance estimated
that revenue lost through this form of piracy amounted to US$4.8bn in Western Europe alone in 1994. There are lots of examples: in 1995, two Swedish students were caught sending copied software packages (Microsoft Word, etc.) over the Internet at the rate of about 150 a day – costing the various publishers close to US$2m. However, this is really part of a broader copyright problem – one that the World Intellectual Property Organisation (WIPO) is trying to address with proposals to strengthen the Berne and other international conventions.

**Contamination:** This occurs when systems connected to the Net are infected by viruses. As with hacking, the motive may or may not be financial but it creates opportunities for blackmail.

**The virus problem**

The problem came to public attention in 1988 when a Cornell student created a so-called “worm”, a virus that can jam systems by endlessly replicating itself. This was introduced to the Internet’s precursor, ARPANET, and is estimated to have caused about US $90m of damage to 60,000 terminals. This was the first recorded incident of Internet crime – even though the student apparently meant no harm. The first successful UK virus-related prosecution was in May 1995 when the so-called “Black Baron” (a 26 year-old unemployed man from Exeter) pleaded guilty to 11 charges relating to two viruses called Pathogen and Queeg.

In neither of these cases does financial gain seem to have been the motive. Some incidents are almost comic: a major computer manufacturer had its global networks shut down in 1995 because an electronic Christmas card automatically replicated and mailed itself out to everyone listed in an electronic address book. Nevertheless, comic or not, great damage can be done.

**There are two further types of Internet abuse** which, while not themselves crimes, make the Internet well-suited as a medium for them.

- **Conspiracy:** This can be defined as the use of the Net as a means of (international) command, communication and recruitment for illegal purposes. The threat can be directed at targeted members of society (e.g. by sects) or society as a whole (e.g. terrorism), or it can be drug-related. There is no hard evidence that it is happening, but terrorist groups such as Hezbollah and the IRA might use the Internet to bypass government censorship and threaten society. There are certainly pro-IRA Web sites in the US as well as Web sites serving extremist groups. Even Peru’s Tupac Amaru rebel group has its own home page, as do Mexico’s Zapatistas and the Kurdish Workers Party. Clearly, the Net lends itself to the exchange of coded messages among terrorist networks and drug syndicates.

- **Money laundering:** Moving the proceeds of crime around the world is not possible on the Net in a physical sense, but it does provide a way to transfer notional balances. This would facilitate the exchange and performance of illicit goods/services in one location against an agreed consideration (illicit
or otherwise) in another. Underground banking systems based on physical tokens and money substitutes (e.g. a US$10 bill marked to make it worth US$100,000 in criminal circles) have long existed. The move to passing disguised promissory notes through the Internet is technically very easy, even though it exposes the criminal to the very risks this chapter addresses.

It is worth remembering that both these activities may be carried out by criminals using the Net sites of honest firms and individuals.

A word should be added about persecution of individuals or companies via the Net – an activity on the borderline of legality for which there is some evidence. Sotheby’s, for instance, took legal action in 1995 against the dissatisfied seller of a vintage car who had set up a spoof of the company’s Web site and allegedly used it to badmouth the company to potential clients. Similarly, at the end of 1996, the Labour Party’s Web site was entered and mischievous changes were made to texts and pictures.

There have also been documented cases of what is called “spamming” or “swamping”. The best-known example was in 1994 when a husband and wife law firm in Phoenix, Arizona, angered the Internet user community by posting junk mail notices on 9,000 bulletin boards and discussion groups used by non-commercial and educational bodies. Because of the way the systems were organised, several hundred thousand users inadvertently downloaded the advertisement (which was a solicitation for immigration business). In retaliation, the law firm was multiple messaged, which jammed up its Internet site. However, the last laugh may have been with the lawyers who claimed they still got over US $50,000 of new business.

Notwithstanding all the above, a central finding of our group was that the victims of Internet crime, particularly in the financial sector, feel most vulnerable to reputational damage and loss of confidence in their systems, regardless of the direct economic losses they might suffer. Since this fear is common to all forms of Internet crime, it is not even necessary for a perpetrator to break into a system to do real harm: he merely has to convince the victim that he has the capability to do so.

Victims of crimes on the Internet: Three principal groups can be identified:

- **Direct victims**: owners and operators of systems whose software and data are attacked via the Net. They may also be threatened with follow-up attacks and with the unauthorised use of their data. On top of the direct costs of the attack, they may have to bear the expense of checking how their systems were breached. Their subsequent security and insurance costs are likely to go up, and, most importantly for the financial sector, their reputation may be damaged. This category includes people who receive threats to their persons and non-computer property through the Internet. Not surprisingly, perhaps, it is hard to find individuals or institutions to put into this category. However, Citicorp (which went public with breaches of its security) was
The Internet and Financial Services

one, though it did not go to the authorities until it had first called in private investigators to ascertain the extent of the damage. It will be interesting to see whether the decision to publicise the attempted fraud acted as a deterrent to further attacks.

- **Indirect victims**: individuals or companies who suffer because information about them is illegally obtained from third party data processing or storage facilities. They may have to pay to prevent the data being disseminated or passed on to competitors, to avoid bad publicity or to protect other data. Such victims may not even be Net users themselves. There is no reliable evidence on how many exist.

- **Unwitting victims**: people whose systems are put to illegal use by employees or third parties. They suffer a breach of system integrity and could be sued for negligence. There is scarcely a university or computer lab that is not an unwitting victim in this way. By extension, this group includes firms who risk having compromising material downloaded onto their systems, making them unwitting hosts to criminal activity or potential blackmail victims. It also includes ISPs who suffer from the activities of paedophile “chat groups”.

**Perpetrators of crimes via the Internet**: Perpetrators may be groups or individuals, acting on a planned or opportunistic basis, from inside or outside the target organisation.

The classic perpetrator is the hacker, who may operate from home, office, university, computer laboratory etc, and who (thanks to the miracle of connectivity) does not even have to be physically in the same country as his target, and can operate via a mobile phone.

A great deal of mythology surrounds hackers. Almost all are male, many are socially dysfunctional, but an increasing number of them know that they possess potentially lucrative skills. The challenge for a hacker is to see how far he can go from his own keyboard. The answer is a long way: the attacks on the DoD’s Rome labs were routed through several Latin American countries before they entered the US; some attacks even went via Latvia. It was reported in mid-1996 that US hackers had penetrated Scotland Yard’s PBX system, and had run up over £1m of international calls relating to their domestic hacking activities.

Although hackers tend to be solitary, they like to spread the word and disseminate the tricks of the trade. Indeed, hackers are surprisingly well-organised. There are many fora, physical and electronic, in which they can meet (a 1996 conference organised in London by the University of Westminster provided one such gathering). They also publish glossy magazines, and have on-line publications of which the most important, *Phrack*, has been going since 1985.

*Phrack* is a phenomenon. Widely thought to have been put out of business in the early 1990s, it is still going strong, providing information on computing
systems, networks and telephone systems. Issue 45, published in 1996, included:

- a detailed description of how to hack the Argentine phone system;
- a more discursive piece on the hacking scene in Australia (including applicable laws and the fate of convicted hackers); and
- a description of ways round the Greek telephone system.

Issue 48, published in September 1996, had information on Motorola command mode, Tandy cellular phones and electronic telephone cards. More bizarre, it also had several pages of US legalese asserting copyright and disclaiming responsibility for the content.

Many “hacker boards” are also accessible via the Internet or via private telephone connections. These enable the semi-competent hacker to download codes and/or programmes to break into virtually all commercial software packages and register them without paying.

Hacking has become very sophisticated and hackers’ tools more user-friendly. A good example is the notorious SATAN program (Security Administrator Tool for Analysing Networks) which was released over the Internet in April 1995. SATAN is ostensibly a legitimate tool to enable operators to check their computer systems for weaknesses, e.g. back doors, access parameters etc. But, since it is freely available on the Net complete with documentation, it has also become a hacker’s weapon. Unfortunately, it is a complex program which, if incorrectly used, can damage the systems it is checking. Moreover, SATAN is not alone. Even more advanced programs are now available on the Net some of which can gain an intruder root access to networks and allow him to read and tamper with data. And, just to ensure we all sleep soundly, a 200-page Hacker’s Handbook is available on the Net, having been withdrawn from UK bookshops in 1990 after pressure from the police.

But the “classic” hacker, romanticised in the 1980 Hollywood film, War Games, is not the only threat. Our working group also identified the danger of attacks by:

- **Organised groups**: Carefully planned attacks via the Internet often involve organised syndicates attempting to break into systems to make fraudulent payments or steal confidential information. The means of entry might be obtained from corrupt IT professionals, with bribery financed by, say, drug money. Planning and execution might take months or even years, with accomplices placed in the target organisation. (The Italian Mafia, for instance, allegedly tried to get its own programmers involved in the development of SWIFT.) This pattern is associated with crime originating in the Middle and Far East, and North America. It is also increasingly associated with drug money from Latin America.

- **Ad hoc groups**: These groups tend to attack using cruder methods, including threats of violence, to obtain the confidential systems information they need,
The Internet and Financial Services

or for blackmail and extortion. This pattern is often associated with crime originating in the former Soviet Union.

Scale of the problem: As we have already indicated, it is difficult to obtain reliable data about Internet-related crime. One of the few sources is the GAO study already referred to (though, since one of its purposes was to persuade Congress to vote more money to protect DoD systems from IT threats, it is also suspect). The DoD has 2.1m computers, 10,000 Local Area Networks and 100 long distance networks. The study claimed:

- there had been up to 250,000 attempts a year at penetration;
- a “success rate” of 65% for attempts (defined as getting through at least one layer of security);
- a detection rate by the DoD of only one in every 150 attacks;
- a detection rate of only 4% for those attempts that were successful;
- a disturbing unwillingness, even in the DoD, to report successful attacks that were detected (the study claimed that 73% of successful attacks that were detected went unreported);
- a high cost of investigation (US$500,000 for one particular investigation); and
- a particular susceptibility to attack through connections on the Internet.

If attacks in the business sector are of the same order and carry the same success rate, the problem is very real indeed – and, bearing in mind the value of lost assets and reputation, exceedingly costly. It is also difficult to see, even when it is under one’s nose. According to the Computer Crime Unit at Scotland Yard, a “victim” will often only discover that his system has been compromised when the police tell him – and even then the systems operator will probably deny that penetration is possible.

Contributing factors: Our working group identified several factors which contribute to the growth of Internet-related crime:

- Ignorance: The problem is not just failure to understand the implications of being on the Net, but also to realise when a system is under attack. Such attacks are not always apparent (for example ‘sniffing’ or eavesdropping for passwords), or may initially appear to be a normal breakdown. Few small companies have the resources to detect unwanted attention. Even large systems may merely record these events rather than inhibit them.

- Availability of technology: Sophisticated technology which facilitates crime on the Internet is now available – even in relatively poor countries where people have a strong incentive to obtain data for financial gain. The GAO report says that 120 countries are working on Internet access technology and a great deal of talent is available, particularly in the former Soviet Union and India. Moreover, as a chart presented to the Senate Committee
on Investigations makes clear, the technical knowledge that intruders require has actually fallen with the increased sophistication of the available tools.

**Computer crime clearing house**

Because there is so little evidence on how much computer crime takes place, the CSFI has proposed a new initiative. At present, UK financial firms are under no obligation to report breaches of computer security unless they are material, and there are good reasons why they are reluctant to do so:

- Reputational risk – banks, in particular, fear the bad publicity that goes with exposure.
- A fear that publicising computer fraud will encourage others to test one’s system.
- There is a reluctance to lose face with competitors, which is what would happen if it were known that one particular institution had been ripped off.

The result is that there is no objective measure of whether computer crime is big or small, or whether it constitutes a serious danger. Nor is there any assessment of where the threat is coming from, who the hackers are or what their motivation is. As important, there is no “early warning” procedure; there is no way in which experience can be disseminated to others so that they can take preventative action. The CSFI, therefore, believes that a case can be made for requiring all regulated financial institutions:

- to inform a central body of all attempts to penetrate or otherwise compromise computer systems; and
- to inform that body of steps taken to counter the intrusion.

That would mean an objective register of computer crime broken down by type, origin, etc. This would enable regulators, auditors and the industry itself to determine:

- the scope and scale of the problem;
- ways in which it is changing over time; and
- appropriate counter-measures.

It would also permit some sort of alert system. For this to win industry support, it is important that:

- financial institutions are confident they will not be identified, and that the data collected will be published without revealing which institutions were involved; and
- the body running the data collection agency is independent of the regulators and auditors, perhaps an industry-led clearing house.

**How would the clearing house be funded?** We believe all parties would have an interest in setting up this sort of body, perhaps with a “sunset clause” to ensure it does not become a permanent bureaucracy. Therefore, it would be reasonable to seek funding from:

- the financial services trade associations (the BBA, the ABI, the BSA, etc);
- the relevant regulators (the Bank of England, SIB and the SROs);
- the auditors; and
- the hardware/software providers.

Provided the regulators required the reporting of all computer violations on a timely basis, data collection would be automatic and the playing field would be level. Anonymity could be guaranteed and the information disclosed would be useful – an early warning system could be crucial.
The Committee’s staff statement said that the latest technological breakthrough, graphical user interfaces, had "given anyone with a computer, a modem and access to the Internet the capability to break into someone else’s computer anywhere in the world".  

- **Lack of consistent regulation**: There are no international standards for Net usage; where national standards exist, they often conflict with one another. For example, there are differences in the responsibilities and liabilities of issuers, service providers and end users of information; legitimate action by one party in one country can, in some situations, create an offence by a different party in another. In attempting to establish jurisdiction, traditional concepts such as physical presence no longer apply, while paradigms of existing offences do not always fit Internet crimes precisely enough to obtain convictions. Indeed, the problem of securing convictions is a serious one. In England, for instance, it is not clear to what extent the 1968 Theft Act covers the unauthorised obtaining of computer information (English law suggests that information, unlike goods, cannot be "stolen"). The Computer Misuse Act has also proved hard to enforce.

- **Lack of self-regulation**: Industry self-regulation is only just emerging, in the UK under the auspices of the ISPA. However, its effectiveness is limited by the fact that UK users can easily access material that is not covered by a voluntary code. In the Net’s borderless world, any attempt to impose tough national standards merely risks driving business elsewhere.

- **Economic factors**: The objective of most firms on the Internet is to make money, not to create costly solutions to problems that may never arise. Moreover, particularly in the investment banking area with its "gunslinger" culture, people may override company policy and implement "solutions"

of their own which improve local results but put the organisation as a whole at risk. For instance, one major UK bank introduced a Local Area Network which was supposed to remain isolated. A recent spot check revealed that nearly 500 unauthorised modems had been connected to it – each one a potentially lethal breach of security.

- **Psychological factors:** For some hackers, a major motivation is exploration and adventure via the Net, and the achievement of a reputation under a popular alias or ‘tag’. This urge should not be underestimated. Regardless of whether hackers really are sad and lonely, success at their trade can bring them international renown and a true sense of power.

### 3. Problem analysis

In general, it appears to the group that (with the relatively trivial exception of “spamming” or “swamping”) the Internet has not yet generated many genuinely *new* forms of crime. For instance, code cracking and forgery share many characteristics, even though they require rather different skills. Principally, *the Net allows electronic variations of old forms of crime*. Indeed, it is possible to identify old crimes as they move to, or are expected to appear on, the Internet.

#### Crime transformation

<table>
<thead>
<tr>
<th>Old</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burglary</td>
<td>Hacking</td>
</tr>
<tr>
<td></td>
<td>(penetrating files in a computer)</td>
</tr>
<tr>
<td>Criminal damage (destroying equipment)</td>
<td>Unauthorized moddication</td>
</tr>
<tr>
<td></td>
<td>(modifying logical contents)</td>
</tr>
<tr>
<td>Arson</td>
<td>Viruses</td>
</tr>
<tr>
<td>False accounting (altering manual ledgers)</td>
<td>Unauthorized access to systems</td>
</tr>
<tr>
<td></td>
<td>(with intent to steal or defraud)</td>
</tr>
<tr>
<td>Forgery (forging signatures &amp; documents)</td>
<td>Code-cracking</td>
</tr>
<tr>
<td></td>
<td>(with intent to steal or defraud)</td>
</tr>
<tr>
<td>Pornography (magazines and films)</td>
<td>Distributing pornographic material</td>
</tr>
<tr>
<td></td>
<td>(via a computer network)</td>
</tr>
<tr>
<td>Blackmail and extortion</td>
<td>Any of the above with demands</td>
</tr>
<tr>
<td></td>
<td>Computer viruses</td>
</tr>
<tr>
<td>Criminal damage (destroying hardware)</td>
<td>Indecent material (children)</td>
</tr>
<tr>
<td></td>
<td>(printed copies, address lists)</td>
</tr>
<tr>
<td></td>
<td>Accessing personal data</td>
</tr>
<tr>
<td></td>
<td>(printed copies)</td>
</tr>
<tr>
<td></td>
<td>Indecent espionage</td>
</tr>
<tr>
<td></td>
<td>(photographs, corruption)</td>
</tr>
<tr>
<td></td>
<td>Theft and fraud</td>
</tr>
<tr>
<td></td>
<td>Security embargo breaking</td>
</tr>
<tr>
<td></td>
<td>Terror</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Financial computer systems (false fronts)</td>
</tr>
<tr>
<td></td>
<td>Illegal transfer of information</td>
</tr>
<tr>
<td></td>
<td>Information warfare</td>
</tr>
</tbody>
</table>

What is new is the freedom that criminals have in an open system, their ability to work undetected and at distance, the lack of a clear regulatory framework and the vast potential for leverage provided by the Net’s expanding global client base.

This suggests three conclusions:

- **Continual growth:** Attacks against systems will grow at least in line with the increase in the number of new Internet sites and users. Particular concern was expressed in the group about new applet-based Java software that
can send back information from systems in which it has been planted. So far, this is no more than a theoretical concern, and the software manufacturers have been quick to plug any holes that have been identified. Nevertheless, it is conceivable that Java could act as a “Trojan horse” – a program that appears to be something other than it is. This is particularly dangerous since most firewalls are designed to be outward-facing (i.e. to prevent external access). “Trojan horses” could be activated in the middle of the night to trawl their host for data and send out the results by e-mail. These would not be picked up by the firewalls because they were already “inside the castle”.

- **Perpetual leap-frogging**: Hacking and protective skills will continue to develop in competition with each other and it seems unlikely that one will establish an insurmountable lead over the other.

- **Business on closed systems**: Until participants accept a certain level of insecurity as normal (which is the case with other business mediums), high-value business is likely to take place principally on closed, intranet systems.

### 4. Response

Internet crime is an extension of computer crime – a hot topic and the subject of much investigation. So far, however, this has not produced measures which could seriously dent illegal activity.

**International**

At the widest level, the Internet is a focus of the UN’s UNOJUST project. The G-7’s Financial Action Task Force and the Interpol Working Group on Computer Crime are also looking at Internet crime. In early 1996, Interpol and the US authorities co-sponsored a meeting in San Francisco that brought together financial intelligence units (FIUs) from 16 countries and their counterparts from 19 others. The FIUs themselves now cooperate through the so-called “Fighting Group”, which was set up in June 1995 in Brussels. At the request of the G-10, the Bank for International Settlements has also begun to consider the issue, primarily in connection with e-cash.

**Within the EU**, the Internet is being looked at closely by several DGs, though none is focusing specifically on crime except in the context of child pornography and nuclear secrets. A paper on ways of combating these types of crime was sent to the Council of Ministers at the end of last year.

**But all of this sounds better than it is.** In reality, very little of substance is being achieved at an international level to counter advanced forms of Internet crime.

**Government**

Responses at this level vary widely.

**In the US**, banks are obliged to report all deposits of US $5,000 or more – giving them a handle on organised crime. From April 1996, they have also been required to report “suspicious activity” to the Financial Crime Enforcement Network (FinCen) which operates a database in Detroit. By June 1996,
FinCen had not received any reports of computer intrusion, probably because banks prefer to risk the maximum US $5,000 fine for failure to report than admit that their computers were broken into.

As a result, Washington has been reluctant to let industry deal with the matter itself. Although the FBI has set up International Computer Crime Squads in several US cities, the government's primary defence against Net misuse has been its control of encryption technology, most notably restrictions on the use of extended keys, especially outside its jurisdiction. However, this tends to result in less secure systems and conflict between business (which needs strong encryption) and law enforcement (which fears that it could be used to thwart surveillance). This polarisation has fuelled a debate on free speech and civil liberties on the Net. However, these arguments relate mainly to non-financial use of the Net. Where financial security is at stake, bona fide financial institutions (including non-US firms) have been allowed to use the relevant technology.

US consumer groups are also starting to use the Web creatively. For instance, in a joint venture with Canada, the National Consumers' League has set up a Fraud Information Centre (http://www.echotech.com). This has a variety of links to government sites, hacker boards, and computer security firms - as well as to a host of law enforcement agencies throughout the world. It also has salutary examples of current scams.

**Fraud Information Centre**

The following cautionary tale was flagged on the US/Canadian consumer Web site in February 1997:

"Consumers who visited a pornographic Web site (www.sexygirls.com) last month got a big surprise on their phone bills. After a few teaser pictures, the surfer was told he/she needed to download a special program to view the archived images. That program was actually a viewer with an entire communications suite hidden deep inside (a non-self-propagating Trojan Horse). The program disconnected the user from his/her ISP, shut off the volume on the modem if it was computer controlled, and dialled a number in Moldavia. All the while the consumer was on the Web site, and even if he/she then browsed other sites on the World Wide Web, the Internet access was being provided through the Moldavia number, resulting in huge international phone charges! Consumers didn't know that until their phone bills arrived. According to the Toronto Star Business Reporter, there are Canadian reports of bills into the thousands."

**Salutary examples of scams**

In the UK, there appears to be a reluctance on the part of the authorities to introduce specific legislation on Net crime - though some Internet-related issues may be addressed in the next Criminal Justice Bill and/or amendments to the Data Protection Act. The present position seems to be that existing legislation (notably the Computer Misuse Act 1990) is sufficient to handle most types of specific computer crime, and that other relevant legislation (e.g. the Child Protection Act) would extend to Internet offences.
The Internet and Financial Services

As for the UK police response, responsibility for investigating computer crime lies with the force in whose area the crime is reported, and the investigation is assigned to the unit which has the remit for the type of crime involved — usually fraud or vice. There is a national programme to ensure that every police force has officers who are trained to investigate computer crime. Nevertheless, the Computer Crime Unit at the Metropolitan Police Force is the only specialist unit dedicated to investigating offences under the Computer Misuse Act 1990.

In addition:

- the Home Office Action Against Crime Unit has the lead role in the fight against computer crime among government departments;
- the Association of Chief Police Officers has a working group on computer crime that monitors national cyber-crime statistics and is responsible for making policy recommendations to individual police forces; and
- the National Criminal Intelligence Service provides strategic analysis of crime trends in the cyber-crime area.

As noted, ISPA has been in discussion with Scotland Yard about Internet crime, and has set up an Internet Watch Foundation. Several universities are also analysing cybercrime, in particular Loughborough and the University of Wales in Cardiff.

Among the regulators, the Securities and Investments Board has taken the highest profile. The Bank of England keeps a watching brief through its fraud unit, but does not believe that the Internet poses a sufficient threat to require a more active role at this stage.

The initial industry response to Net crime has been low: to date, co-operation on the Net has mainly been at the level of resolving name disputes. ISPA has published proposals for a two-tier self-regulatory system, but these have been criticised as an attempt to shift responsibility from providers to users. This can be partly explained by the fact that transactions wholly over the Net are uncommon, and the main emphasis thus far has been on the Net as an advertising medium. However, certain interest groups have set up working parties to make recommendations to members. For example, British universities follow the UK Education and Research Networking Association’s recommendations — but they do little more, on the grounds that it is impractical to try to control the Net.

Individual companies are developing a belated awareness of the need to protect their systems and avoid becoming unwitting crime victims (e.g. through an employee storing porn on a PC). However, many company policies are implemented without regard to their enforceability or proper monitoring facilities.

Some companies pass the problem on to consultants and accountants. There is also increasing interest in insuring against losses from computer crime, though this has the disadvantage of compensating for damage rather than preventing it, and encouraging the notion of an ‘acceptable’ level of crime. This cost,
which is largely passed on to consumers, ends up supporting a whole class of criminal activity.

Other countries take various approaches. In some, what is not forbidden is allowed, which results in a permissive regime. In others (e.g. China, Saudi Arabia and Singapore) comprehensive legal and administrative steps have been taken to censor all Net traffic.

How secure is secure? In preparing this book, an interesting difference of view emerged between the security and crime working groups. The security group took the view that technology (sensibly applied) could provide an acceptable level of security, largely through cryptography. But the crime group thought that, strictly speaking, there is no security on the Internet. Any amount of protection can be developed and installed, but it provides no guarantee that the system will be secure. That said, some operating systems are inherently more vulnerable than others. Ironically, open architecture UNIX-based systems are easier to penetrate than older, more primitive systems, while the introduction of Java as the programming language of choice may add another level of vulnerability (though, to be fair, attempts to break the Java system have so far failed).

The main forms of security being used today include:

- **Firewalls and anti-virus programmes**, which are intended to block intrusions or prevent inside users from exceeding their authorisations. These are becoming increasingly sophisticated, e.g. the Sidewinder system. They are also becoming ubiquitous: Dr Solomon (a UK manufacturer of anti-virus protection programmes) was one of the first companies to float on the Alternative Investment Market. But firewalls only offer protection against attack from the outside; they may be vulnerable to hostile programmes that have been inadvertently imported.

- **Cryptography**, which will become increasingly powerful as the US authorises the export of larger keys, but which can be used by criminals as well as against them.

- **Standard security protocols**, which affect the organisational context in which security breaches occur – e.g. how are they reported? and what is done about them?

Unfortunately, the group has ample evidence that all three approaches can be, and are being, compromised – regardless of the technological sophistication of the victim.

Civil remedies are also available for victims, though most are of little practical use. For instance, funds transferred illegally may be traced and recovered through the civil courts. But this is a time-consuming and expensive exercise, particularly in cases with an international dimension. Injunctions can also be obtained but, if the identity of the person to be enjoined is not known, service of the injunction can be difficult. (However, in one UK case, the court was
The Internet and Financial Services

prepared to accept service by e-mail at the address of the defendant since this was the only way he could be identified.)

The group concluded, therefore, that the current response to crime on the Net is generally incomplete and/or ineffective. The rapid pace of development – combined with confusion in regulation and the lack of industry, technological and procedural standards – is a major obstacle. Of even greater concern is the relatively low importance placed on Internet crime by the authorities – except when it involves terrorism or paedophilia. Generally, legislators and enforcers have other priorities: in Europe, for example, drugs and immigration. Moreover, in the absence of distinct legislation, the authorities are often unwilling to offer detailed advice on improving Internet security as it might lead to liability. This does not encourage security planning at levels which permit economies of scale.

Security specialists: Not surprisingly, the combination of a real threat, the lack of hard data and an inadequate official response has prompted a large number of private sector companies to jump into the field – with some success, as Citicorp’s call on private investigators showed.

Companies providing assistance in the prevention and investigation of computer crime fall into three main categories:

- **Accountancy and IT consultancy firms**: These include the IT consultancy arms of the Big Six accountancy firms and the IT consultancy houses themselves, such as Andersen Consulting, Coopers & Lybrand, Ernst & Young, Price Waterhouse, Deloitte & Touche, Cap Gemini, Computer Management Group, Logica, and SEMA. KPMG has gone as far as to establish an international Internet Penetration Laboratory in Palo Alto, California.

- **Software and hardware providers**: Computer and software manufacturers have a vested interest in ensuring the integrity of their products and assisting with the weaknesses of others’.

- **Specialists**: A number of specialist companies provide advice on specific problems and problem areas. Security companies such as Kroll, Control Risks, Group 4 and Securicor have all branched into computer security from their bases in the physical security and asset recovery business. Several UK companies also offer highly focused assistance on crime prevention and investigation. Three such firms were represented in the group preparing this chapter – Compliance Methodology Consultants, Computer Crime Consultants, and Maple Network Consultancy.

Given the complex legal and jurisdictional issues involved, several major law firms are active in this field. Among the bigger UK practices, Lovell White Durrant was represented in the group.

Self-help: Despite the growing availability of security services, the working group felt that the biggest contribution to the fight against computer/Internet
crime must come from greater awareness and better procedures at individual company level. The fast-moving Net environment means that crime prevention must be a continuous process of risk monitoring and assessment on the one hand and implementing risk prevention measures on the other. The Net is already host to a large number of (generally low grade) criminal acts, and more serious crimes are certain to be committed in the future, especially if large volumes of business are transacted over the Net.

It is worth re-emphasising that many companies that believe they are not connected to the Internet are vulnerable because they can still be accessed over telephone lines.

**Nailing the hackers**

**The problem of evidence:** One of the obstacles to prosecuting computer hackers is obtaining sufficient evidence. In the UK, the police have tended to rely on material stored on the hacker's hard disk and other media, but the increased availability of strong cryptography is likely to stop this source. Because much of the evidence is computer-generated, special rules relate to its admissibility in court. Given that hackers may go through several systems before reaching their true target, prosecution can be laborious. The longer the chain, the greater the evidential problem.

The strongest evidence might be a record of the data traffic on a suspect's phone line. But while the police can obtain a warrant to tap a telephone, the evidence can only be used for intelligence gathering, not in a court of law. Even the suggestion that a warrant was issued is so prejudicial that it cannot be hinted at by prosecution or defence. Therefore the police have been deprived of a powerful weapon; instead, they have to rely on limited information provided by call loggers.

Similar problems arise in other jurisdictions. In a recent US case, the authorities were unable to trace certain hackers beyond the system they were using as a staging platform. To do so required a Federal warrant - which they were doubtful they would obtain - so they had to rely on old fashioned informants.

**Catching the criminal:** The problems of obtaining admissible evidence are nothing compared to catching the hacker in the first place. It may be possible to trace a hacker back to the point from which he is dialling in. But most hackers cross many systems (and ISPs) in different countries to cover their tracks, even if the target is just across the road. The problem is even greater if the hacker has "gone mobile", using cloned mobile phones. While it is possible to trace a mobile phone to the cell where it is being used, this only gives a general indication of the caller's location. Tracking is possible, but it is difficult and assumes that the hacker is fairly fixed. Serious hackers do not operate from home but are constantly on the move.

Given the international dimension to this problem, cross-border co-operation is vital. This has improved greatly at the European level in the last few years, largely through the efforts of John Austen, the former head of the Computer Crime Unit at Scotland Yard. However many barriers still exist - language being but one.
5. Conclusions and recommendations
The group reached the following broad conclusions about crime and the Internet:

- Net users will inevitably be exposed to crime and the seriousness of that crime will probably be linked to the importance of the underlying business.
- Although the Internet itself will not give rise to many new forms of crime, it will make some "old" crimes much more of a threat.
- Given the inevitable lag between Internet crime and legislative and police response, users will have to take action themselves to avoid being direct or indirect victims and possibly unwitting offenders.
- Initially, users must set their own standards both internally and externally in collaboration with other users.
- In the absence of concerted official policing, crime prevention will rely to a large extent on the sharing of information about crime and anti-crime measures.
- Prevention will have to be paid for, though its cost is low both absolutely and relative to the scale of potential damage.
- The best prevention is built into systems rather than added on as an afterthought.

Finally, the group makes the following recommendations:

- Clearer regulation.
- Better education on technical matters.
- Better screening of IT staff/privileged users.
- A more detailed understanding of IT risks by insurers.
- More action at an industry level – both informal reporting and, perhaps, more formal requirements.
- More resources for enforcers and investigative agencies.
- More education on ethical issues at school, college and on the job.
- Specialist IT courts and better training for judges.
- Stiffer penalties, especially to permit confiscation of equipment.
## GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2BCD</td>
<td>The European Union’s Second Banking Co-ordination Directive.</td>
</tr>
<tr>
<td>Active-X</td>
<td>Alternative to Java applets for Microsoft Explorer browsers.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>The mathematical formula that underlies the process of encrypting data. A systematic procedure for solving mathematical problems in a finite number of steps.</td>
</tr>
<tr>
<td>AOL</td>
<td>America On Line. A subscriber computer network, principally in the US, aimed at the retail user and providing a number of on-line facilities, including access to the Internet.</td>
</tr>
<tr>
<td>Applet</td>
<td>A small, self-contained software program which is downloaded to a computer to execute a specific function. It is then erased or otherwise not stored on the computer on which it was executed. Also referred to as a &quot;Java applet&quot;.</td>
</tr>
<tr>
<td>ARPA</td>
<td>Advanced Research Projects Agency, run by the US Department of Defense.</td>
</tr>
<tr>
<td>BACS</td>
<td>Bankers Automated Clearing System. The UK’s system for automated mass banking payments.</td>
</tr>
<tr>
<td>Bean</td>
<td>Alternative name for a small “applet”.</td>
</tr>
<tr>
<td>Beta test</td>
<td>Final phase of testing a new or revised software program where a large number of users are asked to try the software and report any shortcomings or “bugs” to the developer.</td>
</tr>
<tr>
<td>Boolean logic</td>
<td>Type of formal logic used to define sets.</td>
</tr>
<tr>
<td>Browser</td>
<td>A software package used to access the Internet – particularly the WWW – via an Internet service provider or subscriber computer network.</td>
</tr>
<tr>
<td>CCITT</td>
<td>Comité Consultatif International de Télégraphique et Téléphonique. Institution responsible for developing international standards in data transmission.</td>
</tr>
<tr>
<td>CERN</td>
<td>Conseil Européen pour la Recherche Nucléaire, known today as the European Laboratory for Particle Physics.</td>
</tr>
<tr>
<td>Clipper chip</td>
<td>Encryption chip used in EES which allows a “back door” into anything it is used to encrypt.</td>
</tr>
<tr>
<td><strong>CLMI</strong></td>
<td>Commercial Lines Marketing Initiative. A system of electronic trading standards for commercial insurance.</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Closed network</strong></td>
<td>A computer network without external dial-in capabilities, i.e. where one cannot log-on to the network from a remote location. If such a system is based on HTML technologies, it can be referred to as an “intranet”.</td>
</tr>
<tr>
<td><strong>CoCom</strong></td>
<td>Co-ordinating Committee for Multilateral Export Controls.</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td>A situation in which a computer is, or has the ability to be, connected to one or more other computers.</td>
</tr>
<tr>
<td><strong>Converter</strong></td>
<td>Program for conversion of message formats, e.g. from EDIFACT into a user-specific format.</td>
</tr>
<tr>
<td><strong>Cryptoanalysis</strong></td>
<td>The art of breaking cyphers.</td>
</tr>
<tr>
<td><strong>Cryptography</strong></td>
<td>The science of keeping messages secret.</td>
</tr>
<tr>
<td><strong>Cryptology</strong></td>
<td>The study of the mathematical foundations of cryptographic methods.</td>
</tr>
<tr>
<td><strong>Cypher</strong></td>
<td>General name for any method of encryption and decryption.</td>
</tr>
<tr>
<td><strong>Cyphertext</strong></td>
<td>The text of an encrypted message.</td>
</tr>
<tr>
<td><strong>Data format</strong></td>
<td>Structure of a file and data segments contained in it. SWIFT, ODETTE, VDA and EDIFACT are data formats with which electronic data interchange can be conducted.</td>
</tr>
<tr>
<td><strong>Data segment</strong></td>
<td>A record consisting of functionally related data elements identified by their sequence in the record. A segment begins with a segment tag and ends with the segment-end-character.</td>
</tr>
<tr>
<td><strong>DES algorithm</strong></td>
<td>Symmetrical encryption algorithm. US standard since 1977, and widely used internationally.</td>
</tr>
<tr>
<td><strong>DG</strong></td>
<td>Directorate General (of the EU).</td>
</tr>
<tr>
<td><strong>DigiCash</strong></td>
<td>Technology for e-cash on the Internet spearheaded by a Dutch company.</td>
</tr>
<tr>
<td><strong>EEA</strong></td>
<td>European Economic Area (i.e. EU plus Norway and Iceland).</td>
</tr>
<tr>
<td><strong>E-cash</strong></td>
<td>General term to describe electronic money, i.e. money which is non-physical in nature and used principally in on-line transactions.</td>
</tr>
<tr>
<td><strong>E-mail</strong></td>
<td>Electronic mail. Messages received or sent by electronic means over computer networks, especially the Internet.</td>
</tr>
<tr>
<td><strong>ECE</strong></td>
<td>See UN/ECE.</td>
</tr>
<tr>
<td><strong>EDGAR</strong></td>
<td>Electronic Data Gathering, Analysis and Retrieval. The SEC’s computer system for company filings.</td>
</tr>
<tr>
<td><strong>EDI</strong></td>
<td>Electronic Data Interchange. General term for transmission of business data in a standardised format between different EDP systems.</td>
</tr>
</tbody>
</table>
EDIFACT
Electronic Data Interchange for Administration, Commerce and Transport. EDI standards developed by UN/ECE WP4 and now ratified by the ISO. EDIFACT was developed as the framework for a national and international syntax and for specific message formats.

EDIFICE

EDP
Electronic Data Processing.

EES
Escrow Encryption Standard, proposed in 1993 by the Clinton Administration. This includes the Clipper Chip, an encryption technique which effectively contains a “back door” to enable government agencies to eavesdrop on its users. As a result, the technology is freely exportable from the US.

EFT
Electronic Funds Transfer.

Egmont Group
An informal organisation, set up in June 1995 in Brussels, through which the financial intelligence units of various law enforcement agencies cooperate.

EPS
On-line trading system used in the insurance industry.

EU
European Union.

Euro ISDN
Euro ISDN is a successor to the Integrated Service Digital Network (ISDN). It is part of an effort to standardise ISDNs for Europe on the basis of a new “D-channel” protocol.

FinCen
Financial Crime Enforcement Network.

FIU
Financial Intelligence Unit.

FIX
A trading protocol that was devised in 1993 to support a connectivity project between Fidelity and Salomon Brothers. It has since been expanded to cover most trading software vendors in both New York and London (where it was introduced in mid-1996).

FSA

G-7
Group of Seven. Top seven industrialised countries in the world.

G-10
Group of Ten. Top ten industrialised countries in the world.

G-20
A group of US and European commercial banks involved in setting up a proprietary clearing system.

Gateway
PC, mainframe computer or specialised hardware acting as an access or through point to a further computer, which itself can be networked or stand-alone.

GUI
Graphical user interface.
<table>
<thead>
<tr>
<th><strong>Hash function</strong></th>
<th>Process in which data is compressed to produce tamper-proof encrypted messages. Used for electronic signatures.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hits</strong></td>
<td>Numerical value defining the number of times a Web site is accessed. A Web page having 100 “hits” a day implies that the page is accessed by 100 WWW users per day.</td>
</tr>
<tr>
<td><strong>Home page</strong></td>
<td>The main Web page of an organisation with a Web presence. Often used as the starting point for navigation within a given organisation’s site.</td>
</tr>
<tr>
<td><strong>Hypertext link</strong></td>
<td>Text or picture on a Web page which, if clicked, brings the user to a different location on the <a href="http://WWW">WWW</a>. In essence it is an HTML function used to link WWW sites and pages together.</td>
</tr>
<tr>
<td><strong>HTML</strong></td>
<td>Hyper-text mark-up language. Language used for creating pages, connections, etc. on the WWW.</td>
</tr>
<tr>
<td><strong>http</strong></td>
<td>Hyper text transfer protocol.</td>
</tr>
<tr>
<td><strong>IOSCO</strong></td>
<td>International Organisation of Securities Commissions (based in Montreal).</td>
</tr>
<tr>
<td><strong>IFA</strong></td>
<td>Independent financial adviser</td>
</tr>
<tr>
<td><strong>Intelligent agents</strong></td>
<td>Software which functions in an “intelligent” fashion, that is, by noticing patterns of activity, having learning capabilities, etc. Often used to search for specific information on the Internet.</td>
</tr>
<tr>
<td><strong>Intranets</strong></td>
<td>A closed network using HTML technology standards.</td>
</tr>
<tr>
<td><strong>IPO</strong></td>
<td>Initial public offering.</td>
</tr>
<tr>
<td><strong>Internet Service Provider</strong></td>
<td>See ISP</td>
</tr>
<tr>
<td><strong>ISO</strong></td>
<td>International Standards Organisation. Institution responsible for developing international standards in data transmission.</td>
</tr>
<tr>
<td><strong>ISP</strong></td>
<td>Internet Service Provider. A company in the business of providing access to the Internet for end users (corporate or private).</td>
</tr>
<tr>
<td><strong>ISPA</strong></td>
<td>International association for ISPs.</td>
</tr>
<tr>
<td><strong>ITAR</strong></td>
<td>International Traffic in Arms Regulations.</td>
</tr>
<tr>
<td><strong>Java</strong></td>
<td>Special computer language developed by Sun Microsystems which allows software programs to be stored in a central location and accessed by other computers only as and when required. Such software programs are also known as “Java applets”.</td>
</tr>
<tr>
<td><strong>JEPI</strong></td>
<td>Joint Electronic Payments Initiative. Established by W³C and CommerceNet to provide a universal payment platform allowing merchants and consumers to transact business over the Internet using many different forms of payment.</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>LIMNET</strong></td>
<td>London Insurance Market Network. A joint venture between four market bodies (LIRMA, ILU, Lloyd's and LIBC) to use technology to improve the efficiency of the London insurance market.</td>
</tr>
<tr>
<td><strong>Link page</strong></td>
<td>A Web page specifically designed to contain links to Web pages of a particular kind. It is an alternative to search engines for locating information on the WWW.</td>
</tr>
<tr>
<td><strong>Local area network</strong></td>
<td>Computer network covering a limited user area, e.g. usually a single floor, room, department or building within an organisation.</td>
</tr>
<tr>
<td><strong>Message</strong></td>
<td>A set of data subdivided into sections and exchanged between two partners in EDI. Also called “document” or “transaction set”.</td>
</tr>
<tr>
<td><strong>Modem</strong></td>
<td>Modulator-Demodulator. Device which transforms digital computer signals into analogue signals (and vice-versa), used to allow computers to communicate with each other over telephone lines.</td>
</tr>
<tr>
<td><strong>Mondex</strong></td>
<td>A proprietary technology for electronic money, on the Internet and otherwise, initially developed by NatWest Bank.</td>
</tr>
<tr>
<td><strong>Net surfer</strong></td>
<td>One who uses the WWW on a regular basis. Also applied to describe people with considerable expertise in Internet technologies and navigation techniques.</td>
</tr>
<tr>
<td><strong>Net surfing</strong></td>
<td>Exploring the WWW by use of links between Web pages (specially applicable if done without the use of search engines).</td>
</tr>
<tr>
<td><strong>Networked</strong></td>
<td>Status of a PC or mainframe computer when it is connected to one or more other PCs or mainframe computers.</td>
</tr>
<tr>
<td><strong>Neural net</strong></td>
<td>Mathematical methodology attempting to reproduce synoptic patterns of the brain in an effort to solve complex pattern recognition problems in mathematics and other fields.</td>
</tr>
<tr>
<td><strong>ODETTE</strong></td>
<td>Organisation for Data Exchange through Teletransmission in Europe. Responsible for developing message standards and file transfer protocols in the automotive industry; also an EDI message standard for the European car industry.</td>
</tr>
<tr>
<td><strong>OGEL(x)</strong></td>
<td>Open General Export Licence. Under UK export regulations an OGEL(x) is needed to export goods which provide access control and/or authentication, or which are specially designed for banking transactions.</td>
</tr>
<tr>
<td><strong>Open standard</strong></td>
<td>Hardware or software protocol which is generally available to anyone wishing to adopt it. There may be licensing agreements and/or fees payable for its use to the protocol's developer/owner.</td>
</tr>
<tr>
<td><strong>Open system</strong></td>
<td>Hardware or software system/protocol or which is generally available to the public. Sometimes incorrectly used to mean &quot;open standard&quot;.</td>
</tr>
<tr>
<td><strong>ORIGO</strong></td>
<td>A joint venture between a group of insurance companies and AT&amp;T to provide quotations for insurance products as a proprietary on-line service.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>Card inserted to increase a computer's functions.</td>
</tr>
<tr>
<td>PGP</td>
<td>&quot;Pretty good privacy&quot;. An encryption technique of which, despite trying, the US government has not managed to halt the export.</td>
</tr>
<tr>
<td>Plaintext</td>
<td>Terminology used in the computer security industry to indicate a non-encrypted message.</td>
</tr>
<tr>
<td>PEP</td>
<td>Personal Equity Plan.</td>
</tr>
<tr>
<td>Polaris</td>
<td>Polaris was formed by seven insurers in 1994 to introduce standards for electronic trading in the insurance industry. A PC-based software tool called ProductWriter has been developed by Polaris to provide insurers with the ability to define their products and send electronic trading messages.</td>
</tr>
<tr>
<td>POS</td>
<td>Point-of-sale.</td>
</tr>
<tr>
<td>Proprietary system</td>
<td>Hardware or software system/protocol which is owned by an organisation and not generally available to the public. Sometimes incorrectly used to mean a &quot;closed network&quot;.</td>
</tr>
<tr>
<td>RSA algorithm</td>
<td>Asymmetrical cryptographical algorithm. RSA is the algorithm normally used to generate digital signatures. It is also commonly used for the distribution of secret keys. RSA Corp. is now a major player in the encryption business. (RSA stands for its inventors - Rivest, Shamir and Adelman.)</td>
</tr>
<tr>
<td>SATAN</td>
<td>Security Administrator Tool for Analysing Networks. Released over the Internet in April 1995, it is a tool to enable operators to check their computer systems for security weaknesses. It is regularly abused by hackers.</td>
</tr>
<tr>
<td>SCORs</td>
<td>Small Corporate Offering Registrations. Individual US state-regulated stock issues that enable issuers and investors to cut out the commissions that investment banks usually charge on IPOs.</td>
</tr>
<tr>
<td>Search engine</td>
<td>An on or off-line facility or software package for retrieving information from the Internet.</td>
</tr>
<tr>
<td>SET</td>
<td>Secure Electronic Transaction. A protocol created by MasterCard and Visa designed to make credit card payments over the Internet more secure. Piloted in late 1996, and expected to become widely available in 1997.</td>
</tr>
<tr>
<td>Server</td>
<td>Computer hardware specifically used and/or designed to act as gateway to other computers. Often acts as a central repository of shared files in a LAN.</td>
</tr>
<tr>
<td>Spider</td>
<td>A program which maps Internet sites in an automated fashion, reporting back to its owner all relevant information requested. If badly written, it can cause severe damage to the sites it scans.</td>
</tr>
<tr>
<td>Stand-alone</td>
<td>State of a PC or mainframe computer when it is not connected to any other PC or mainframe computer (in any way).</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stand-alone dial-up</td>
<td>Non-networked PC with a modem, using a standard telephone line to connect to either PCs or networks.</td>
</tr>
<tr>
<td>Store-and-forward</td>
<td>Message transfer procedure with temporary storage until final recipient is able to receive it.</td>
</tr>
<tr>
<td>SWIFT</td>
<td>Society for World-wide Interbank Financial Telecommunication. A widely used inter-bank wholesale payment and settlement system.</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>A single standard protocol for communication between computers. It is the basis on which the Internet is founded.</td>
</tr>
<tr>
<td>Telnet</td>
<td>Part of the Internet which allows access to Internet linked computers on a direct basis.</td>
</tr>
<tr>
<td>TTP</td>
<td>Trusted Third Party.</td>
</tr>
<tr>
<td>UCITS</td>
<td>Undertaking for Collective Investment in Transferable Securities. This creates a single market in Europe for the cross-border promotion of open-ended collective investment undertakings which invest in transferable securities (i.e. mutual funds).</td>
</tr>
<tr>
<td>UN/ECE</td>
<td>United Nations Economic Commission for Europe. Authority in charge of various European EDI initiatives, e.g. EDIFACT.</td>
</tr>
<tr>
<td>UNGTDI</td>
<td>Computer communications standard used in the insurance industry, and in particular by Brokernet. Less widely-adopted than EDIFACT standards.</td>
</tr>
<tr>
<td>UPP</td>
<td>Universal Payment Preamble. Negotiations protocol that identifies appropriate payment methodology.</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator. Address (location) of a WWW page or Internet document.</td>
</tr>
<tr>
<td>VANS</td>
<td>Value Added Network Systems.</td>
</tr>
<tr>
<td>Wide area network</td>
<td>Computer network covering a large user area. Such a network is usually composed of a number of sub-networks, each in a different geographical/office location.</td>
</tr>
<tr>
<td>WIN</td>
<td>World-wide Insurance Network. It will be available to all insurance brokers and insurance companies world-wide, and will provide a secure, customised and manageable communication system. The project’s backers are Alexander &amp; Alexander, Aon, Johnson &amp; Higgins, Marsh &amp; McLennan, Sedgwick and Willis Corroon.</td>
</tr>
<tr>
<td>WP4</td>
<td>Working Party 4 of UN/ECE. Works on the simplification of international trade rules.</td>
</tr>
<tr>
<td>World Wide Web (WWW)</td>
<td>Graphics driven part of the Internet developed by CERN laboratories in 1991. It is primarily responsible for the growth of the Internet’s popularity.</td>
</tr>
</tbody>
</table>
The following CSFI papers are also available from the Centre:

**FINANCING THE RUSSIAN SAFETY NET** *by Peter Ackerman/Edward Balls*
A proposal to fund employment benefit in Russia through the sale of bonds to Western investors. £40

**DERIVATIVES FOR THE RETAIL CLIENT** *by Andrew Dobson*
How derivative instruments might be adapted for use by the retail customer to reduce risk. £20

**RATING ENVIRONMENTAL RISK** *by David Lascelles*
A scheme to rate companies according to their ability to handle their environmental liabilities. £25

**ELECTRONIC SHARE DEALING FOR THE PRIVATE INVESTOR** *by Paul Laird*
Using electronic media to supply stockbroking services directly to small investors. £25/$40

**THE IBM DOLLAR** *by Edward de Bono*
How large corporations can issue their own currency. £15

**UK FINANCIAL SUPERVISION: A BLUEPRINT FOR CHANGE** *by Andrew Hilton*
A controversial proposal for amalgamating and rationalizing supervision of financial services. £25

**BANKING BANANA SKINS**
Five leading commentators examine the risks facing banks in the current economic cycle. £25

**A NEW APPROACH TO CAPITAL ADEQUACY FOR BANKS** *by Charles Taylor*
A new and radical approach to setting capital levels, by the rapporteur of the G-30 report on derivatives. £35

**NEW FORMS OF EURO-ARAB COOPERATION** *by Jacques Roger-Machart*
Creating a Euro-Arab investment company to stimulate European investment in the Arab world. £25

**BANKING BANANA SKINS II**
Four leading UK bankers and a senior corporate treasurer discuss lessons for the future from the last banking crisis. £25

**IBM/CSFI PRIZE: TECHNOLOGY AND FINANCIAL SERVICES 1994.**
**PRIZE-WINNING ESSAYS**
Two prize-winning essays. £10

**LIQUIDITY RATINGS FOR BONDS** *by Ian Mackintosh*
A proposal to rate bond issues for liquidity. £25

**BANKS AS PROVIDERS OF INFORMATION SECURITY SERVICES** *by Nick Collin*
Banks have a privileged position as transmitters of secure data: they should make a business of it. £25

**AN ENVIRONMENTAL RISK RATING FOR SCOTTISH NUCLEAR** *by David Lascelles*
An experimental rating of a nuclear utility. £25
ECONOMIC AND MONETARY UNION STAGE III: THE ISSUES FOR BANKS
by Malcolm Levitt
Banks may be underestimating the impact of Maastricht’s small print. £25

BRINGING MARKET-DRIVEN REGULATION TO EUROPEAN BANKING:
A PROPOSAL FOR 100 PER CENT CROSS-GUARANTEES by Bert Ely
A proposal for eliminating systemic banking risk by using cross-guarantees. £25

THE CITY UNDER THREAT by Patrick de Jacquelot
A leading French journalist worries about complacency in the City of London. £20

THE UK BUILDING SOCIETIES: DO THEY HAVE A FUTURE?
A collection of essays by leading commentators (sponsored by the Alliance & Leicester). £20

OPTIONS AND CURRENCY INTERVENTION by Charles R Taylor
A proposal for using an option programme to defend exchange rate targets. £25

TWIN PEAKS: A REGULATORY STRUCTURE FOR THE NEW CENTURY
by Michael Taylor
A proposal for restructuring UK financial regulation around systemic and conduct-of-business roles. £25

BANKING BANANA SKINS III
The results of a questionnaire, sent to senior financial figures in the UK and abroad, asking where the next problems for the banking industry are likely to emerge. £25

WELFARE: A RADICAL RETHINK – THE PERSONAL WELFARE PLAN
by Andrew Dobson
A proposal to create a privately funded alternative for the full range of welfare provision. £25

“PEAK PRACTICE”: HOW TO REFORM THE UK’S REGULATORY STRUCTURE
by Michael Taylor
Putting “Twin Peaks” into practice. £25

CENTRAL BANK INTERVENTION: A NEW APPROACH by Neil Record
A radical approach to central bank intervention – without foreign exchange reserves. £25

THE CRASH OF 2003: AN EMU FAIRY TALE by David Lascelles
An all too plausible scenario of what might happen if EMU precedes economic convergence. £25

BANKING BANANA SKINS: 1997
Another annual survey of worries about the financial system. £25
The Centre receives general support from the following institutions:

Abbey National
Andersen Consulting
Barclays Group
Chase Manhattan Bank
Citibank
International Securities Market Association
Merrill Lynch
Price Waterhouse
The Private Bank & Trust Company Limited
Union Bank of Switzerland

Alliance & Leicester
AMS
Corporation of London
Cityforum
Cripps Sears Transearch
Deutsche Morgan Grenfell
DTI Innovation Unit
EMI Group
Fidelity Brokerage
Guardian Royal Exchange
HM Treasury
ICL/Fujitsu
ITT, Bombay
KPMG Management Consulting
Linklaters & Paines
Lloyds TSB
Lloyd's of London
London Stock Exchange

Morgan Stanley International
National Westminster Bank
PA Consulting
Rockport Financial
Royal Bank of Scotland
Salomon Brothers Asset Management
Société Générale
Standard & Poor's Ratings Group
Sun Life Assurance
Visa International

Australian Association of Permanent Building Societies
Arthur Andersen & Co.
BDO Stoy Hayward
Bank of England
British Invisibles
Brigade Electronics
Brown Brothers Harriman
Ernst & Young
Extel Financial
Guinness Mahon
Halifax Building Society
IBCA
JP Chown & Co.
Gerrard & National/Lombard Street Research
Mercury Communications
Schroders
Standard Chartered Bank

In addition, the Centre receives special purpose support from, among others, the British Bankers' Association, EBRD, the ESRC, Global Asset Management, Hambros Bank, IBM, IMI/Sigeco, LIBA, Lovell White Durrant, ODA, Observatoire de la Finance, Pearson Professional, The Banker, Saudi International Bank, SRI International, the World Bank Group, and the World Gold Council.
| A | AAA Investment Guide 66  
ABN Amro 46  
Access A&A 53, 86  
Active-X 69, 104  
Admiral Insurance 78  
Advanced Research Projects Agency 6  
Aeon 87  
Aequus 70  
ALG Europe 82  
Alexander & Alexander 83, 87  
Alexander Houlden Group 73, 83  
Ali4One 67  
Allied Dunbar 62  
Altavista 63, 65, 66, 67  
America Online 7  
Andersen Consulting 31, 68, 89, 103, 104  
AOL 35, 45, 95  
Apollo Trust Company 62  
Arch 6  
ARPANET 6  
Artelms 86  
Association of Investment Trust Companies 57, 64  
Association of Unit Trusts and Investment Funds 57  
AT&T 21, 36, 49, 71  
ATM 36, 49  
Austin Reed 59  
Automobile Association 78  
AutoNomy 68  
AXA 78  |
| B | Bacon & Woodrow 53  
BACS 137, 143, 155  
BAH 46  
bancassurance 12  
BarcOne 46  
Bank for International Settlements 145, 192  
Bank of England 48, 109, 120, 152, 183, 189, 194  
Bank of Scotland 31, 47, 60  
BankAmerica 46, 62  
Bankers Trust 64  
Banking Act 1987 109, 120, 121  
Baran, Paul 6  
Barclays Bank 60, 62, 78  
Barclays Stockbrokers 53, 89  
Barclay Square 17, 47, 48, 50, 59  
BargainFinder 68, 103  
Barnett 46  
Barrow's 91, 95  
BBC World Service 31, 53, 177  |
| C | Benfield's 83  
Bermuda 73, 86, 88  
Berners-Lee, Tim 6, 143  
Bigfoot 67  
BITNET 6  
Bloomberg 89, 99, 100, 102, 109  
Booz, Allen & Hamilton 18, 45, 46, 47, 50, 91, 92  
British insurance & Investment Brokers Association 78  
British Telecom 39  
Brockbank Underwriting 73, 80, 86  
Brokernet 77  
BrokerPlus 104  
BSkyB 103  
BT 137, 153  
Buckingham Gate 17, 48, 50, 59  
Business Software Alliance 183  
Business Technology Network 53  |
| D | Cap Gemini 137  
CAS 21  
Centre for Accountability and Debt Relief 177  
CERN 6  
certificate registry 43  
certification 150  
certification authority 21, 33, 43  
Champion Consulting 105  
Channel Islands 121  
CHAPS 146  
Chase Manhattan 46  
Chatham Insurance 78  
chat rooms 101, 182, 183  
Child Protection Act 1993  
China 195  
Chitty on Contracts 127  
Churchill 78  
Cisco 172  
Citelles 47  
Citibank 45, 46  
Citcorp 34, 182, 185  
Clarinet 7  
Clifford Chance 86, 105, 137  
Clipper Chip 114  
CLM 77  
COCOM 114  
Commercial Union 79  
Comptroller of the Currency 156  
Compuserve 7, 35, 48, 95, 182  
Computer crime clearing house 189  
Computer Crime Unit 177, 188, 194, 197  
Computer Misuse Act 190, 193, 194  
Computer Security Institute 180  
Computer Weekly 35, 36, 37  |
The Internet and Financial Services

DTI Innovation Unit 53
Duttacher 55
Duttacher Multimedia Ltd 7

E
E*trade 92, 95, 96, 97, 99
e-cash 20, 21, 28, 98, 120, 123, 124, 134
e-mail 6, 7, 11, 22
e.Schwab 96, 97, 99
EDIFACT 77, 147
Egmont Group 192
electronic contracts 26
electronic data interchange 77
Electronic Fund Transfer Act of 1978 124
electronic purse 39, 52
Empire Financial 95
encryption 10, 15, 20, 26, 27, 29, 109, 113, 114, 129, 130, 141, 149, 150, 155, 163, 164, 165, 166, 167, 168, 171, 175
envelope cryptography 113
EPS 81
Ernst & Young 31, 53
Escrow Encryption Standard 114
ESI 31, 53, 89
esponage 114
EU Directive on data protection 126
European Commission 114
European Economic Area 122
European Parliament 114
European Union Bank 48
Eurostar 59
Excite 67
Ezra-Weinstein, Ben 92

F
FarSight 95
FBI 180, 193
Federal Reserve 34, 123
Fidelity 46, 62, 65, 66, 96, 97, 103
Financial Centre 64
Financial Crime Enforcement Network 192
Financial Services Act of 1986 115, 134
Financial Times 8, 31, 45, 64, 70, 95, 183
FIND 62
Find an IFA 57, 70
Findex 54
Firefly Network 68
firewalls 155, 160, 162, 170, 172, 175, 192, 195
First Chicago NBD 46
First Direct 40
First Virtual 17, 137, 149
FIX 103
Flemings 57
Forrester Research 40, 49
Fortuna Alliance 182
France Telecom 47
fraud 177, 179, 180, 182, 186, 189, 193, 194
FreeLoader 68
Friends Provident 62
FSA 115, 119
Fundscape 64

G
G-7 192
Gaella 70
GAM 57
Gartmore 57
Gates, Bill 36
GATT 114
GE 36
General Accident 79
Global Asset Management 64
Global On-line Directory 67
GlobalAccess 101
Gopher 6
Guardian Insurance 79
Guthall Ltd 103, 165, 177

H
hacker 177, 181, 182, 186, 187, 193, 197
Hacker’s Handbook 187
Hacking 183, 187, 192
hacking 26, 27, 181, 183, 184, 186, 187, 192
Halifax 62
Herzog Heine Geduld 95
Hiscox 79, 80, 86
Home Office Banking Service 47
HSBC 137
HSBC Gibbs Benefit Consulting 53
HSBC Holdings 105, 137, 177
HSBC/Midland 62
HTML 7, 37, 60, 69, 91, 102, 104, 147
hyper-text markup language 7
Hyperion 31, 137

I
IBM 31, 46, 82, 137, 141, 143, 146
ICL 48, 137, 155
IFA 18, 57, 70, 71
IFA Association 70
IFA networks 70
IFAs 53, 57, 64, 69, 70, 72
ILU 82
IMRO 71, 102, 132
independent financial adviser 70
information 18, 85
information warfare 179, 181
Infospace 67
Innovative Customer Systems 89
 Integral Development 137, 148
Integration 46

I
intelligent agents 12, 27, 56, 68, 69, 84, 103, 113
Interactive Investor 57, 59, 64, 69, 70
International Association for Financial Planning 70
International Chamber of Commerce 134
International Data Corp 93
International Traffic in Arms Regulations 165
Internet Explorer 63
Internet Service Providers Association 182
Interpol 192
Interpretation Act 1988 129
InterSure 79
Intranet 10, 13, 179, 180, 192
Intuit 19, 45, 46, 48, 174
Investec 64
Investment Services Directive 122
Investorama 59, 62, 64, 69
IOSCO 23
IPONet 92
ISMA Centre 89
ISPA 182, 193, 194
ITT Quotec 77

J
Java 61, 69, 103, 104, 162
Java "applets" 15, 41
Java "beans" 44
JEPI 137, 143
Johnson, Rick 68
Johnson & Higgins 83, 87

K
Kew Association 35, 37
key escrow 26, 27, 164, 167, 168, 169
King, Mervyn 152
Kleinwort Benson Investments 105
KPMG 105
KTQ Consulting 137

L
Large, Sir Andrew 25
Lauric 135
legacy systems 33, 102
LBA 137
UBC 82
Liberty 89
JR Licklider 6
Lifestylefinder 68
LIFFE 105
LIMNET 81, 82
link pages 15, 53, 68, 69, 70, 72, 160
Lincoln National 79
Linklaters & Paines 53, 89, 105
LIRMA 82

212
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lloyd's 73, 76, 82, 86</td>
</tr>
<tr>
<td>Lloyd's TSB 48</td>
</tr>
<tr>
<td>Lombard Street Research 89</td>
</tr>
<tr>
<td>London Business School 53</td>
</tr>
<tr>
<td>London Clearing House 137</td>
</tr>
<tr>
<td>London School of Economics 89</td>
</tr>
<tr>
<td>London Stock Exchange 93, 94</td>
</tr>
<tr>
<td>Los Angeles Times 183</td>
</tr>
<tr>
<td>Loughborough University 177</td>
</tr>
<tr>
<td>Lovell White Durant</td>
</tr>
<tr>
<td>31, 53, 105, 177, 196</td>
</tr>
<tr>
<td>Lycos 63, 67</td>
</tr>
<tr>
<td>M</td>
</tr>
<tr>
<td>M&amp;G 57, 86, 155</td>
</tr>
<tr>
<td>macropayments 40</td>
</tr>
<tr>
<td>Mafia 187</td>
</tr>
<tr>
<td>Managing Your Money 46</td>
</tr>
<tr>
<td>Maple Network Consultancy 156</td>
</tr>
<tr>
<td>Mark Twain Bank 46</td>
</tr>
<tr>
<td>Market manipulation 183</td>
</tr>
<tr>
<td>market manipulation 183</td>
</tr>
<tr>
<td>MarketWatch 100</td>
</tr>
<tr>
<td>Marks &amp; Spencer 41</td>
</tr>
<tr>
<td>Marsh &amp; McLennan 87</td>
</tr>
<tr>
<td>MasterCard 21, 140, 141, 142, 145</td>
</tr>
<tr>
<td>McGinn Stewart &amp; Partners 53, 89</td>
</tr>
<tr>
<td>McKinsey 42</td>
</tr>
<tr>
<td>Mellon 46</td>
</tr>
<tr>
<td>Mercantile and General Re 82</td>
</tr>
<tr>
<td>Mercury Communications 137, 155</td>
</tr>
<tr>
<td>Merrill Lynch 95</td>
</tr>
<tr>
<td>Micropal 64</td>
</tr>
<tr>
<td>Micropayments 40</td>
</tr>
<tr>
<td>Microsoft</td>
</tr>
<tr>
<td>48, 63, 69, 82, 141,</td>
</tr>
<tr>
<td>143, 145, 163, 165, 174</td>
</tr>
<tr>
<td>Microsoft Money 17, 46, 57, 63</td>
</tr>
<tr>
<td>Midland Bank 31, 40</td>
</tr>
<tr>
<td>Millicent 137, 145</td>
</tr>
<tr>
<td>MILNET 6</td>
</tr>
<tr>
<td>Minet Group 105, 177</td>
</tr>
<tr>
<td>Minipayments 40</td>
</tr>
<tr>
<td>Minitel 45, 47</td>
</tr>
<tr>
<td>MondoX</td>
</tr>
<tr>
<td>20, 21, 39, 41, 48, 124,</td>
</tr>
<tr>
<td>137, 143, 144, 145, 153</td>
</tr>
<tr>
<td>money laundering</td>
</tr>
<tr>
<td>129, 177, 179, 184</td>
</tr>
<tr>
<td>MoneyNet 100</td>
</tr>
<tr>
<td>Moneyweb 64</td>
</tr>
<tr>
<td>MoneyWorld 59, 62, 69, 70</td>
</tr>
<tr>
<td>Morgan Stanley 89, 97, 155</td>
</tr>
<tr>
<td>MSi Global Inc 64</td>
</tr>
<tr>
<td>Myths 77</td>
</tr>
<tr>
<td>N</td>
</tr>
<tr>
<td>Nanopayments 40</td>
</tr>
<tr>
<td>NASDAQ 92, 93</td>
</tr>
<tr>
<td>National Australia Group 60</td>
</tr>
<tr>
<td>National Criminal Intelligence Service 154</td>
</tr>
<tr>
<td>National Security Agency 167</td>
</tr>
<tr>
<td>NationsBank 46</td>
</tr>
<tr>
<td>Nationwide 60</td>
</tr>
<tr>
<td>NatWest 48, 50, 62, 165</td>
</tr>
<tr>
<td>Navigator 65</td>
</tr>
<tr>
<td>Nelson Media 55</td>
</tr>
<tr>
<td>Netscape</td>
</tr>
<tr>
<td>27, 47, 48, 69, 125, 141,</td>
</tr>
<tr>
<td>142, 153, 165, 172, 174</td>
</tr>
<tr>
<td>neural network 68, 95</td>
</tr>
<tr>
<td>New York Stock Exchange 93</td>
</tr>
<tr>
<td>Northern Rock 60</td>
</tr>
<tr>
<td>Norwich Union 60, 66, 70, 79</td>
</tr>
<tr>
<td>NSFNET 6</td>
</tr>
<tr>
<td>Numa Financial Systems 64</td>
</tr>
<tr>
<td>O</td>
</tr>
<tr>
<td>OECD 165</td>
</tr>
<tr>
<td>Omnium Communications</td>
</tr>
<tr>
<td>Limited 62</td>
</tr>
<tr>
<td>Ono 71</td>
</tr>
<tr>
<td>P</td>
</tr>
<tr>
<td>PA Consulting Group 31, 137</td>
</tr>
<tr>
<td>Pacific Coast Brokerage 91, 96, 97</td>
</tr>
<tr>
<td>packet-switching 5</td>
</tr>
<tr>
<td>paedophile 182, 186</td>
</tr>
<tr>
<td>paedophilia 196</td>
</tr>
<tr>
<td>Pearl Assurance 60, 79</td>
</tr>
<tr>
<td>PEP 57, 65, 66</td>
</tr>
<tr>
<td>Pharos Consulting 53</td>
</tr>
<tr>
<td>PSIP 114</td>
</tr>
<tr>
<td>Price 186</td>
</tr>
<tr>
<td>PIA 71, 102, 132</td>
</tr>
<tr>
<td>Pipex 7</td>
</tr>
<tr>
<td>Polaris 77</td>
</tr>
<tr>
<td>PolicyMaster 77</td>
</tr>
<tr>
<td>pornography 179, 182, 192</td>
</tr>
<tr>
<td>Preferred Direct 79</td>
</tr>
<tr>
<td>Price Waterhouse 31, 89</td>
</tr>
<tr>
<td>&quot;prime bank&quot; securities 183</td>
</tr>
<tr>
<td>ProductWitter 77</td>
</tr>
<tr>
<td>Prolific 57</td>
</tr>
<tr>
<td>Proshare 89</td>
</tr>
<tr>
<td>Prospera Direct 79</td>
</tr>
<tr>
<td>Proton 39</td>
</tr>
<tr>
<td>public key cryptography</td>
</tr>
<tr>
<td>163, 164, 165, 168</td>
</tr>
<tr>
<td>Pyramid schemes 182</td>
</tr>
<tr>
<td>Q</td>
</tr>
<tr>
<td>Q-Trade 99</td>
</tr>
<tr>
<td>GBE 82</td>
</tr>
<tr>
<td>Qualiteam 69</td>
</tr>
<tr>
<td>Quicken</td>
</tr>
<tr>
<td>17, 19, 26, 45, 56, 47, 58, 57, 63, 146</td>
</tr>
<tr>
<td>Quick &amp; Reilly 96, 97</td>
</tr>
<tr>
<td>R</td>
</tr>
<tr>
<td>Rabobank 49</td>
</tr>
<tr>
<td>RAND Corporation 6</td>
</tr>
<tr>
<td>Reed, John 34</td>
</tr>
<tr>
<td>relying party 43</td>
</tr>
<tr>
<td>Restrictive Trade Practices Act 1976</td>
</tr>
<tr>
<td>128</td>
</tr>
<tr>
<td>Reuters 100, 102, 109</td>
</tr>
<tr>
<td>RINET 82</td>
</tr>
<tr>
<td>Robertson, Stephens 92</td>
</tr>
<tr>
<td>Robson Rhodes 105</td>
</tr>
<tr>
<td>Royal Bank of Scotland</td>
</tr>
<tr>
<td>17, 48, 60, 79</td>
</tr>
<tr>
<td>Royal Insurance 79</td>
</tr>
<tr>
<td>RSA</td>
</tr>
<tr>
<td>164, 165, 166, 167, 169, 172, 174</td>
</tr>
<tr>
<td>RSA Data Security 141</td>
</tr>
<tr>
<td>S</td>
</tr>
<tr>
<td>Sainsbury 41, 59</td>
</tr>
<tr>
<td>Sainsbury Five 62</td>
</tr>
<tr>
<td>SAITAN 187</td>
</tr>
<tr>
<td>Saudi Arabia 195</td>
</tr>
<tr>
<td>Save the Children 182</td>
</tr>
<tr>
<td>SBC Warburg 155</td>
</tr>
<tr>
<td>Schroders 57, 89</td>
</tr>
<tr>
<td>ScorNet 92</td>
</tr>
<tr>
<td>SCORs 92</td>
</tr>
<tr>
<td>Scotland Yard</td>
</tr>
<tr>
<td>177, 186, 188, 194, 197</td>
</tr>
<tr>
<td>Scottish Amicable 65, 70</td>
</tr>
<tr>
<td>Scottish Provident 70</td>
</tr>
<tr>
<td>search agent 55</td>
</tr>
<tr>
<td>search engines</td>
</tr>
<tr>
<td>53, 63, 65, 67, 68, 69, 70</td>
</tr>
<tr>
<td>Search Voyer 67</td>
</tr>
<tr>
<td>SEC 91, 92, 101, 132, 133</td>
</tr>
<tr>
<td>Second Banking Co-ordination</td>
</tr>
<tr>
<td>Directive 122</td>
</tr>
<tr>
<td>Secure Trust 48</td>
</tr>
<tr>
<td>Securities and Investments Board 25, 115, 116, 194</td>
</tr>
<tr>
<td>security audit 161</td>
</tr>
<tr>
<td>Security First 17</td>
</tr>
<tr>
<td>Security First Network Bank 46, 62</td>
</tr>
<tr>
<td>Sedgwick 83, 87</td>
</tr>
<tr>
<td>SET</td>
</tr>
<tr>
<td>137, 141, 145, 150, 153, 165, 168</td>
</tr>
<tr>
<td>SFA 102</td>
</tr>
<tr>
<td>Sharelink 96, 97, 99</td>
</tr>
<tr>
<td>shareware 67</td>
</tr>
<tr>
<td>sheep dip 162, 170</td>
</tr>
<tr>
<td>SH Systems 31, 73</td>
</tr>
<tr>
<td>SIB</td>
</tr>
<tr>
<td>89, 105, 112, 115,</td>
</tr>
<tr>
<td>132, 137, 177, 189</td>
</tr>
<tr>
<td>Siemens Nikdorf 167</td>
</tr>
<tr>
<td>signing party 43</td>
</tr>
<tr>
<td>Simmons &amp; Simmons 53, 105, 137</td>
</tr>
<tr>
<td>Singapore 195</td>
</tr>
<tr>
<td>software piracy 177, 183</td>
</tr>
<tr>
<td>Dr Solomon 170, 195</td>
</tr>
<tr>
<td>Sotheby's 185</td>
</tr>
<tr>
<td>spiders 68</td>
</tr>
<tr>
<td>Spring Street Brewing 22, 91, 92</td>
</tr>
<tr>
<td>Springman Tipper Campbell 31</td>
</tr>
<tr>
<td>SRT International 53, 155</td>
</tr>
<tr>
<td>SSL 165</td>
</tr>
<tr>
<td>Standard &amp; Poor's 65</td>
</tr>
<tr>
<td>Standard Life 57</td>
</tr>
<tr>
<td>Stock Data Corporation 64</td>
</tr>
<tr>
<td>Sun Alliance 65, 79, 86</td>
</tr>
</tbody>
</table>
The Internet and Financial Services

Sun Life 53
Sun Microsystems 15
SWIFT 166
Swiss Investment Marketplace 64
Swiss Search Engine 67
Symmetric cryptography 163, 164, 165

T
T-Online 45, 47
TCP/IP 6, 161
Telereate 102
Telnet 7
terrorism 179, 184, 196
Tesco 41
The Bankers Network 171
The Bureau 141, 142
The New York Times 94
The Research Department 53
Thief Act 190
Toronto Dominion 62
TrodataPoint 89, 99, 100
Transatlantic Re 82
Transition Partnerships 53, 73
Trojan horses 27, 170
Trust on the Internet 64
Trusted Third Parties 21, 33, 43, 114, 113, 137, 150, 174
TrustWeb 167
TTPs 21
Tucows 67

U
UAP Provincial Insurance 73, 79
UCITS 121, 122
UN 192
Unfair Contract Terms Act 1977 128
Unfair Terms in Consumer Contract Regulations 1994 128
Universal Resource Locators 6
UNIX 161
US Banking Administration Institute 34
US General Accounting Office 181
US Postal Service 21, 43, 169
US Supreme Court 182
USENET 6
UUNet Pipex 141, 142

V
VANS 77
VAI 152
VeriSign 169, 174
Vint Cerf 6
Viren 170
Virgin Direct 58
virus protection 155, 170, 172, 175
viruses 27
Visa 21, 40, 46, 47, 140, 141, 142
Visa Cash 39
Vision in Practice 155, 177

W
WAN 6

Wanadoo 47
Westfalia Agreement 167
Webcrawler 67
Wellington 80
Wells Fargo 42, 45, 62
WhoWhere 67
Willis Corroon 83, 86, 87
WIN 11, 87, 88
WIRE 73, 78, 82
Wit Capital 91, 92
World Insurance Network 11
World Intellectual Property Organization 184
World Wide Web 6, 7
World Wide Web Consortium 143
World-Wide Insurance Network 87
Worldcover 79, 80
worm 184
WREN Group Services 73

Y
Yahoo 63, 67