The use of the Internet as an alternative to paper-based, traditional forms of banking introduces new risks and opportunities for fraud, which will be felt both by banks and their consumers. Is the approach taken in relation to consumer protection in the traditional banking environment effective in the sphere of on-line banking?

Table of Contents

Introduction

- IT Law

Over the last five years the Internet has penetrated the home environment in a way which was previously unimaginable, and that exponential growth is likely to continue[1]. The technology involved has become more user-friendly and hence more accessible, allowing almost anyone to become familiar with the Net. Again looking back over the last five years the main concern of IT lawyers and writers has switched from "Internet pornography" to the need for a "legal framework" to support the growth of electronic commerce. This growth can perhaps be best illustrated by the recently completed "largest electronic commerce transaction"; the sale of a jumbo jet for thirty million dollars over the net[2]. Banks have been quick to recognise that the Internet also has commercial value for them, allowing the provision of banking services through a new, more convenient medium.

- Internet Banks

The *Security First Network Bank* pioneered 'Internet' or 'On-line' banking in the US[3], but surveys now suggest that European banks have become equally if not more involved in the provision of on-line transaction capabilities. A report, by Bluesky International Marketing[4], compared Internet banks in the US with those in eight European countries, showing that the US had only one third the number of Internet banks which the European countries had. Although not illustrative of the actual level of *use* that these services receive, the report shows that European banks have been very quick to tap into this new market. The extent to which the traditional "high-street" banks use the internet varies from very basic single page advertising to what some have termed "advanced cyber-banking"; (extensive transaction capabilities). *Barclays Bank* and *The Royal Bank of Scotland* were the first to provide advanced cyber-banking in the UK. The relatively low start up costs associated with 'dedicated'[5] Internet banks has fuelled the creation of new banks such as *Egg* (a subsidiary of Prudential) and *Smile* (a subsidiary of the Co-operative Bank) which are keen to steal customers from traditional banks. Despite the fact that presently only 8% of the UK public are using the net to manage and monitor their finances, a significant demand has been shown for on-line banking[6] - perhaps this is indicative that a large minority of the population are willing to re-consider the way they bank. New, smaller banks along-with High Street banks are recognising the potential of On-line Banking.

- Why use the Internet for Banking ?

The *Bank of Scotland* pioneered home and office banking in the UK, with their HOBS system which was introduced back in 1982. This system gave its users access to the bank's main computer and allowed very limited facilities, (i.e. monitoring of account balances, limited transfer between accounts, some bill payment, etc.). HOBS was initially reliant on dedicated hardware and software and had to charge their customers for both the services and the equipment. The Bank of Scotland continues to retain the HOBS acronym, but they have now focused on the Internet as the ideal medium for this service.

---

[1] Example: Nua Internet consultancy, estimate 179m were online worldwide by June 1999.
[2] (Note: to qualify as an electronic commerce transaction no paper can move between the parties until the goods are delivered).
[3] Opened October 18, 1995 – first full service on-line bank.
[4] Bluesky Report, *Internet Retail Banking in Europe – The New Competitive Landscape*, (1st Nov. 1998).
[5] I.e. the bank has no branch network, but will usually have phone support and a central administration centre.
[6] Statistics*: Datamonitor management consultants.* See also: *NOP research for Marketing*, March 1999. (Survey showed less than 1% currently bank over the internet, but 24% would be prepared to do so)

- Advantages

The Internet has provided a perfect "universally accepted" platform from which to provide home banking services. The main advantages of Internet banking are clear. Firstly, for banks the low "transaction" cost of Internet based operations combined with the greater profitability achievable from Internet users both serve to make Internet banking economically attractive. This advantage is passed on to the consumer who will often benefit from the bank's savings through improved, cheaper and more profitable services.

Secondly, convenience is a major selling factor. For banks, their services and advertisements can be accessed 24 hours a day, 7 days a week and for consumers they are no longer restricted by limited bank branch opening hours. Consumers can bank at any time day or night and do not have to be geographically close to a branch to bank.

Thirdly, the consumer has more control over their finances. Consumers can have instant access to the status of their accounts. The Internet allows the user to make "what if" type calculations, for example: when contemplating taking out a loan the user can assess how such a move would affect his or her finances. The aforementioned advantages are not exhaustive – but are perhaps the main attractions of Internet banking. Unfortunately, banking this way necessitates the transfer of personal, sensitive information that can result in new opportunities for fraud and new risks.

- Disadvantages

Presently the main concern of those contemplating using Internet banking services is "security". The protection of data that various "Encryption" techniques provide is the subject of much discussion, given that the Internet infrastructure allows third parties to intercept communications relatively easily.

Another, perhaps less widely discussed problem is that of 'system overload'. The unforeseen growth in Internet use, (mentioned earlier), puts pressure on the networks throughout the globe. The slowing of network operations at peak use times is indicative of the pressure put on the connections that the Internet utilises.

Many bank customers, (particularly corporations) are not yet using the Internet for banking; this causes the convenience of the medium to be slightly restricted for those that are on-line. For example payments cannot be made on-line if the payee is not also banking on-line.

Additionally, the classic problem is that you cannot obtain cash from a PC, so home-PC transaction capabilities are limited.

From the above brief introduction it should be clear that the Internet is a valuable forum for the provision of banking services, yet it is not without its drawbacks. The purpose of this paper is to look at Internet banking and its regulation from a consumer perspective. To answer the question posed it will be necessary to look at the medium itself, providing a background for a general overview of the risks and problems encountered when transacting by electronic means. Combining banking and the Net was tested firstly in the US – the UK has been fairly quick to follow suit. Reviewing the background to Internet banking will allow a further analysis of the more specific problems encountered when banking and the Internet are brought together. The paper will then focus on the regulations in place and more particularly what they provide for the consumer. The regulation in this area is a complex mix of banking, financial services and data protection legislation. The situation created by the mass of different provisions has been referred to as a "potential legal nightmare"[7]. Additionally it will be necessary to consider 'proposed' legislation and its likely impact on the consumer. In order to limit what is a vast area of law, the paper will focus essentially on Internet banking services directed at UK residents.

The Internet Medium

- System Structure

By definition the Internet is boundary-less, being a network of networks covering the globe

[7] Cristopher Stoakes, *Litany of rules that lag on-line banking*, (Euromoney, Aug. 1999).

with packets of data flowing almost randomly between nodes or terminals. The Internet has its foundations within the US military system. Some 30 years ago military officials wished to create a telecommunications system that would operate despite nuclear attack. The first "Internet" originally operated with just four terminals. If one terminal link went down, (or was attacked), then the message would get to its destination through a different route. The system recognises any sort of limitation or censorship as an obstacle (or attack) and ultimately makes its way around it. Such a structure illustrates the Internet's unsuitability for national regulation, leading many to advocate only global regulation.

- Development

Over the years the Internet was developed mainly by academics who used it as a discussion forum, subsequent to it being opened up commercially. In the early stages the main commercial use of the Net was just for advertising.

Electronic commerce was the next stage, with large-scale buying and selling becoming a reality over the net. Through electronic commerce the Internet has facilitated the growth of a multi billion-dollar industry. Low overheads and easy and convenient public access have been instrumental to the huge growth in this sector. The software giant "Microsoft" is itself recognising the potential of Internet Banking, consulting with High Street banks in an effort to launch an Internet banking section for their Microsoft Network (MSN) site, named 'The Finance Channel'.

- Regulation

The success of the unregulated development of the Internet has led some proponents of the Internet to resist regulation entirely; it is seen as being unduly restrictive. Indeed, the unsuitability of applying traditional regulations to this medium is a recurring theme in discussions about the future of electronic commerce. Providers of web services are largely free to operate as they wish, although they must observe technical rules and Internet protocols.

The lack of any boundaries in this global network is can be advantageous in that important information can be made available around the world in seconds. It also means that web-site operators have, in theory, a limitless potential consumer market. However, the infrastructure of the Internet raises legal jurisdiction issues. With sites being accessible anywhere in the world – Internet traders need to consider whether they need to direct their services towards customers based in a particular territory and to consider the various national rules they may need to observe to avoid transactions being invalidated.

- Security Issues

The anonymity that the Internet allows makes its users particularly vulnerable to fraudulent acts. As we have witnessed an exponential growth in the use of the Internet, so too have we seen a growth in fraud and web-site attacks. Increasing pressure on banks and other businesses to have a Net presence is forcing a growth in the amount of confidential information accessible over the Internet. Consumers also appear more willing to submit personal details over the Net. Such data types are the main targets of fraudsters and hackers. Sites relating to banking and insurance are particularly susceptible to attack, by their nature they handle the transfer of particularly valuable data.

"The number of successful web-site attacks is growing at an alarming rate, by approximately a factor of four each year. The reality of being on-line is that you will always be susceptible to some form of attack. Any security mechanism is going to have some sort of weakness"[8].

Hacking of financially valuable information is a computer crime that is likely to be of increasing relevance into the year 2000. This assertion is backed up by recently completed research[9] into forms of computer crime. The National Criminal Intelligence Service (NCIS) stated that in the future "hacking for information with financial value" is likely to become more commonplace. The report also stated that "Cyber-crimes" have risen from 12000 in 1997 to more than 40000 in 1998. The Report does however, point out that the risk from Internet crime does tend to be overstated in the media; adverse publicity which no-doubt concerns those who are considering using the net for banking

[8] Yag Kanani, *KPMG fighting fraud*, (1999).
[9] National Criminal Intelligence Service (NCIS), *Project Trawler*, three year study (96-98) into Internet Crime.

transactions.

The various problems, (unsuitability for regulation, lack of boundaries, security, loss from fraud, etc), outlined above have made certain High-Street banks reluctant to utilise the Internet for banking services. Despite the dangers that banks and consumers may face, the advantages continue to make the medium appealing. Banks are seen to be losing potential customers, (and in some cases existing customers) if they do not provide an advanced Internet service. Recognising the dangers of the Internet is important so that risks can be minimised, and so that important information is not open to attack. Looking at how banks have capitalised on Internet Banking will be valuable in order to provide a background to the problems that have been encountered and how they have been dealt with.

Combining the Internet and Banking

- Internet Presence

It is true to say that **all** banks have an Internet presence of some kind and there is a general movement towards what is sometimes referred to as 'advanced cyberbanking'[10],:"…where customers can transfer money, pay bills and/or buy financial services".

The Bluesky Report categorised the presence which banks have on the Internet into five sections, the most basic being 'brochureware' – where the site is basically an advertisement for services that are available off-line. From here net presence moves up to an 'interactive' site which in addition to advertisements allows some two-way interaction. A loan application[11] may be the subject of such interaction. Potential customers can input a theoretical situation, and the web-site would provide them with their liabilities in such a situation. This could happen either by e-mail, or on the web-site itself with blanks being filled in and a computation being completed. The next level of net presence is 'intermediate cyberbanking', where there may be *limited* customer services, for example the viewing of account balances and statements on-line. From here a far greater interaction is possible; the bank offering a greater number of services and hence falling into the category of "advanced cyberbank".

- Early experience

Canadian banks[12] were some of the first to experiment with the Internet as a delivery channel for banking services. Early research[13] projected large growth in the market and noted that the average Internet customer is projected as being 50% to 250 % more profitable than the average banking customer is. This study expected that 30% of Bank profits could be made from the Internet customer. These results are confirmed by more recent research, which concluded that an Internet transaction costs 10 times less than the equivalent counter transaction. The potential of this market coupled with the increased penetration of the Internet saw UK banks quickly capitalise on this growth area.

- UK banks Internet development

The *Royal Bank of Scotland* (RBOS) and the *Alliance and Leicester* were the first UK banks to provide an Internet based service, which appeared in 1997. The RBOS protected their system with a hybrid of encryption standards, which their IT department were satisfied could not be breached. They also fully integrated their Internet service with existing branch and telephone facilities. Other banks questioned the security of such systems, the *Bank of Scotland* naming "security and control" as issues which they were not 100% satisfied with. The financial services provider: "*Standard Life*", despite having an Internet presence, did not believe the level of security at that time was sufficient for further transactions to be carried out on the net. Although some main name banks were using the net to provide banking services, low consumer confidence and indeed the lower usage of the Internet at this time restricted the success of such services.

---

[10] Bluesky Report, *Internet Retail Banking in Europe – The New Competitive Landscape,* (1st Nov. 1998).
[11] cannot be *completed* on-line, Consumer Credit Act 1974 s.61.
[12] Royal Bank's "*Royal Direct*", Canada Trust's "*EasyWeb*", etc.
[13] Booz-Allen, 1996 (US) survey.

From the initial two main banks, others gradually began to provide full Internet banking, as of the start of this year five main high street banks provided full "advanced cyberbank" services. Even the *Clydesdale bank*, which has generally been sceptical of the security of the medium, is currently in the process of developing a full Internet banking service. Surveys[14] are not in complete agreement as to the precise numbers banking on-line at present, but agree that the number of users will grow dramatically into the next century. This appears indicative that, for today's consumer, the advantages of on-line banking outweigh the risks.

- New Banks

Today's consumer also seems more willing to switch banks. The success of supermarket banks, and newer banks such as *Smile* and *Egg*, shows significant erosion of the importance placed on the reliability/goodwill associated with traditional high street banks. The success of smaller ventures is forcing the older brand name banks to make full use of the latest technology in order to compete with the feature-rich services that newer banks are prepared to offer consumers. The increased profitability which Internet banks can achieve allows them to provide more attractive services, giving the consumer more for their money.

Using the *Egg* bank as an example, its relatively small size when compared to High Street banks allows it to adapt quicker to market developments and to provide new services as soon as they become available. The success[15] of *Egg* reflects the fact that consumers are now willing to shop around for the best deal, (for example in terms of the most favourable interest rates and other fringe benefits). Mike Harris, chief executive of *Egg* has stated that his bank: "…..will be introducing a stream of innovations which will encourage a large permanent switch in personal finance habits."

Despite the area of banking in general being heavily regulated, new banks such as *First-e* are entering the market to compete not only with the newer banks, but also to attract customers of the established High Street banks. *First-e* is Europe's and indeed the UK's first "Internet-only" bank, in that there is no branch network and telephone back up will be limited and will be at extra cost to the consumer. Despite limited resources and a staff of just 250, *First-e* are competing directly with much larger banking groups.

The current situation in the banking arena is that of change. New players are entering the market, and traditional banks have had to come to terms with this new challenge. The result has been a quick move to provide Internet services. The consumer not only wants increased convenience and control, but better services. It is emerging that if these are not offered, the consumer will often be prepared to move banks or invest elsewhere. There is some question as to whether the speed of entrance into the Internet banking forum has been at the expense of proper consumer protection and security. It is obvious from the above that the market is developing at a fast rate, and the attractions to potential customers are growing. To assess the safety of the medium it is necessary to now turn to the problems and legal issues associated with banking on the net. This will be followed by a more detailed look at existing statutory provisions, and new, proposed measures on both a national and European level.

Internet Banking – Specific Problems

- Systematic Barriers

A recent article, "Litany of rules that lag on-line banking"[16] focused in on the problems that banks encounter when putting their services on-line. The problems that banks face are often felt by the consumer. The article referred to the problem of "systematic barriers" that banks encounter; the high level of uncertainty surrounding the legal treatment of electronic transactions is problematic for banks *and* consumers. Banks may find themselves unable to enforce payment obligations contracted over the

[14] Fletcher Research,: currently 200000 users, growth to 7million in 2003. Datamonitor,: currently 450000 users, growth to 2.2 million in 2002. (Figures as at Mar 25, 1999)

[15] £5 billion in deposits, 500000 customers – meeting 5yr target in six months. Latest figures suggest deposits in excess of £7 billion (Source: Financial Mail on Sunday, Jan 2000).

[16] Cristopher Stoakes, *Litany of rules that lag on-line banking,* (Euromoney, Aug. 1999).

net. Customers may find that they are unable to back out of a contract they entered accidentally. Presently, confusion exists as to the legal status of on-line contracts, digital signatures, e-mail, Internet based payment systems, etc. The present regulatory framework for banking does not address *Internet* banking. Due to the absence of new law banks are complying with old regulations applying to normal bank operations, although still in the dark as to their precise applicability. Consumers encounter similar uncertainties concerning the applicability of normal consumer laws. However, the DTI[17] have indicated that electronic commerce will be subject to the same consumer protection legislation as traditional means of shopping. This does not, however, make the Internet banking consumer's legal position much clearer. The DTI guidance is merely indicative of the approach that *should* be taken. Additionally, it is unclear whether Internet banking falls within the DTI's definition of electronic commerce.

Even at the stage of opening an account banks must acquire documents in *hard-copy* form to comply with the Money Laundering Regulations 1993[18]; which provide that there must be procedures by which the applicant provides satisfactory evidence of their identity; otherwise the matter should go no further.

The extent to which these regulations affect the consumer was illustrated by a recently completed investigation[19] into opening bank accounts on-line. *Barclays Bank* and *Smile* accounts required a number of "off-line" formalities to be completed. In both cases, the user had initially to revert to using the phone. As an existing customer with *Barclays* the investigator was able to open an account relatively easily, but with *Smile* a number of documents had to be posted in. Again, the money laundering regulations[20] required that he sent in a utility bill to confirm his address and previous bank statements to prove his financial stability. The current situation is that proof of identity must be given in more than one form on the creation of an account. It is unlikely that a customer will be allowed to prove their identity using only electronic means for a number of years. Despite proposed measures concerning digital signatures (discussed later), there is likely to be some debate as to whether this would open the door to money laundering. For the consumer, a paper-trail will always be necessary initially; before the relative freedom of Internet banking can begin. The British Bankers Association (BBA) gives guidance to Banks on the application of the 1993 Regulations. Along-with identification, banks should have procedures for record keeping and internal reporting, a matter which must be considered in the specification for the structure of Internet banking procedures.

Another example of obeying rules applying to paper based operations serving to restrict Internet banking is shown by the *Royal Bank of Scotland*'s attempt to offer loans on-line. The bank can do this; it can also offer on-line loan approval due to its integration with credit reference agencies. However, total computerisation is not possible – a hand-written signature is required in order to satisfy the Consumer Credit Act[21]. To make the process relatively straightforward the consumer can download the relevant form and add his or her signature later. The consumer must physically post the signed document to the bank. The Act restricts the total convenience which could be achieved by completing the transaction on-line.

The above examples are not really problems, they simply restrict the extent to which banking services can be placed on-line. The above measures have been followed because at present there is no regulation applying specifically to Internet banking services. If there were legislation giving legal effect to such electronic contracts, then the convenience of Internet Banking would be enhanced because a large portion of opening and managing an account could be completed on-line, as could loan applications. Although our previous discussions have shown that the legislative uncertainty is not a barrier to Internet banking, banks are not comfortable with operating in an environment of such uncertainty. Such uncertainty is problematic on a number of levels; it restricts consumer confidence, it lessens the convenience of Internet banking and casts doubt over whether normal remedies could apply.

- Need for *Integrated* service provision

---

[17] DTI – Communications and Information Industries – *Net Benefit: Electonic commerce agenda foe the UK.*

[18] Banks commit an offence if they do not comply, reg. 5.

[19] Jonathan Duffy, *UK Personal Account (Part 1) – Getting Started*, (BBC News On-Line, November 1999).

[20] Identification procedures, regs. 7-11, 1993 regulations.

[21] Consumer Credit Act 1974, must be signed in the prescribed manner by the debtor, (s.61(1)(a)), and by or on behalf of the creditor (s.61(4)). Sections 60-66 concern document rules.

Banks should recognise that they will be unable to "go it alone". As can be seen above on-line loan application is facilitated by *integration* with credit reference agencies. The Bank may have a large IT department, but in order to make a development successful parties such as Internet Service Providers (ISP's), retailers, consultants, etc will have to be involved. The integration of these parties will increase the success of the banking operation, e.g. the consultants will have experience of how to maximise the success of E-commerce operations and larger retailers will allow bank customers to transact directly with them. Additionally, the goodwill and reliability associated with brand name ISP's and retailers will enhance the credibility of the service and will hopefully improve consumer confidence. Experienced consultants and ISP's will have a background of dealing with unauthorised attacks, and hence will be able to advise on where to concentrate protection to minimise risks. Banks have had to deal with the integration requirement before – in relation to shared ATM networks. Integration is not really a problem but a solution – sharing the problems of entering the market lessens the technical burdens that banks face. Where integration does become a problem is in apportioning liability for loss.

- Apportionment of Liability

Liability is a key issue given the ethereal nature of the Internet. With paper transactions it is possible to trace, for example, the payment of a cheque from start to finish – with the balances changing in the accounts of the payee and payer. However, with Internet banking there is a time when the location of the transaction data cannot be identified. The intangible electronic nature of the actual transmission from terminal A to B, or in Internet banking from the customers home PC to the banks main computer, simply cannot be monitored comprehensively. The nature or structure of the World Wide Web, often described as a network of networks, creates innumerable routes which the encrypted data can take from customer to bank. This structure can make it vulnerable to attack from a number of angles.

Stealing or unauthorised appropriation of sensitive data could permit the attacker to pass himself or herself off as a bona-fide customer; an opportunity which could lead to losses for both banks and their customers. This is a scenario that would be impossible to completely eliminate, therefore banks should set-up clear agreements apportioning liability between those in the chain of data passage. As mentioned above, ISP's, consultants, retailers, etc. will be involved in an integrated system. Where possible, it should be set out clearly to the customer and other parties who takes responsibility for particular problems and when such liability attaches. To avoid excessive demands on parties who have no knowledge of the contents of the data they transmit, proposed European legislation[22] has suggested that no liability should attach to parties who are 'mere conduits' of the data. The ethereal nature of the Internet does present new complexities when apportioning liability. There should not be a time when the parties can escape responsibility for the security of the data they process.

- Terms and Conditions

Again, continuing to look at the issue of liability, banks will have to consider the contents and the location on the web-site of the "terms and conditions" attached to their services. This issue is relevant more to Electronic Commerce as opposed to Internet banking; as a matter of normal procedure, the terms and conditions applicable to an account[23] or a credit agreement[24] (a loan) *should* be made available in '*hard copy*' form. In the absence of new law or guidance, banks would be well advised to continue this tradition.

What is actually included within the terms and conditions for the provision of an Internet banking service will vary between banks, and bank accounts. Due to the presently high levels of uncertainty regarding the legal status of various net operations, banks are likely to want to reduce their risks through comprehensive terms and conditions. Although this practice could deal with potential problems, banks would have to ensure that their provisions do not conflict with the Unfair Contract

---

[22] Proposed Electronic Commerce directive, com(98) 586 final, Article 12.

[23] Banks subscribe to the BBA, *Code of Good Banking Practice*, (2nd ed., 1994). Section 4 provides requirements concerning terms and conditions.

[24] S.61(1)(b), Consumer Credit Act 1974 requires that all terms of the agreement, other than the implied terms, are embodied in a document.

Terms Act[25] by making the terms fair and ensuring that they do not remove the consumer's fundamental rights. Given the likely complexity of terms and conditions, consumers would be well advised to study them in detail before entering into any agreements with Internet banks.

From a consumer perspective, it would be advantageous if the terms and conditions were **clearly** available on the site and that there existed the facility to download or print out the terms. If the terms and conditions are available through a "hypertext link" – (perhaps most convenient for the banks), then there is some doubt as to whether courts would agree that the terms were binding. In legal terms, the safest way of presenting the terms and conditions is to have a pre contract web page and a facility whereby the potential customer may scroll through the provisions. Banks, especially when electronic contracts become formally recognised as legally binding, should ensure terms and conditions are made as openly available as they are when contracting "normally", otherwise banks may be unable to rely on their terms.

- Risk form Attack / Fraud.

In a recent article[26] on fraud in the E-commerce industry, consumer risks were divided up into categories. An "investment fraud" was illustrated by the case of a fraudster who created a web-site passing his company off as the next 'Microsoft' and recruited investors, raising $190,000 from 150 investors. The investment was a complete con, and the individual in question pocketed the proceeds. The article made reference also to "Internet Risks", comprising attacks for financial gain. The example given was of a Russian hacker's attack on a US bank system. He managed to transfer funds from customer's accounts into his own account, and was only caught after transferring some $400,000. The success of the attack was due to a small component in the Bank's system which had been replaced without being thoroughly tested – 'carelessness' was the root cause. Although the article centres on E-commerce in general, banks are naturally at a great risk from fraud and other attacks. With the statistics above[27], showing a rise in successful attacks on web-sites, safety procedures should always be followed in order to alleviate the rise in attacks.

In relation to "logging-on" procedures, it is essential that the bank can positively identify the customer. Account holders at the *Co-operative Bank* must register by phone and supply five pieces of personal information such as their mother's maiden name. The customer must enter these five pieces of information each time he or she logs-on to transact. Existing *Barclays bank* customers must apply to use the Internet service by mail, after which they are supplied with a PIN number. This number must be entered along with a password every time the customer logs-on. These details are encrypted before being sent to the bank. The theory is that this will stop hackers from passing themselves off as customers.

Fraud is a problem which Banks are continually battling. Fraudsters have been able to gain access to the money of others through ATM and EFTPOS transactions for some time. Even recent articles[28] label Counterfeit ATM card fraud as a growing problem.

The Internet provides new opportunities for fraud, but it also provides new means to combat such fraud. With the Internet banking customer having greater control and immediate access to their finances - they will be able to identify unauthorised transactions a lot quicker, and hence combat fraudulent transactions.

Banks should carry out "fraud risk assessments" at an early stage. Such assessments would highlight those areas likely to be most vulnerable to attack. Following on from here, measures should be put in place to prevent employee fraud. In many cases the success of an attack is more likely when completed by an insider. As the project nears completion, a stringent set of tests should be carried out – these should draw on information from the risk assessment as well as that from the IT department itself. Banks should take every care to test and better test their systems in order to avoid losses such as those caused by the Russian hacker.

So far we have discussed the background to Internet Banking and the services which banks are

[25] S.15 – 1977 Act provides the contracts governed by the Unfair Contract rules in Scotland.
[26] Alex Plavsic, Tad Dippel, Shabir Hussain, *IT Facilitating fraud,* (International Review of Law, Computers and Technology, August 1999).
[27] See extract by Yag Kanani, KPMG Head of Internet Security, *KPMG fighting fraud,* (1999).
[28] *Banks hit by rise of 32% in counterfeit card fraud,* (Financial Times, March 1999).

presently offering from their web-sites. Identifying the marketplace as an area of rapid change, we then chose to discuss the main problems that had been encountered in the On-line banking field. Whereas some problems originate from the lack of applicable statute law, others are completely new to banks. Given the financial value of data that banks transmit, the risk from fraud was also discussed.

The next logical step is to look at existing legislation and its application to Internet banking. Linking Internet banking and legislation is a difficult task, many provisions are merely *presumed* to apply in the absence of new law. Following on from existing legislation, the paper will look at the measures that the EU and the UK are proposing in order to facilitate the growth of the electronic commerce, and hence Internet banking industries. The multitude of new provisions emerging from both Europe and further afield suggests that amending existing legislative provisions would prove unsatisfactory.

Regulations

- Data Protection legislation

One of the first formal statutes to make specific provision for data held on computers was the Data Protection Act 1984 (1984 Act). All those[29] who process or control personal data must observe those rules set down by the 1984 Act. The Act is due for an update by the 1998 Act of the same name, which implements the European Data Protection Directive.[30] Despite this new act not actually coming into force until mid-2000, it will have retroactive effect and hence banks and others, even now, must observe its provisions. Banks will already be registered under the 1984 Act, but now they must also ensure that their terms of registration include the upload and download of personal information from their web-site. The means by which banks process e-mails should be considered in light of the Data Protection Acts. Whether these are stored or deleted immediately after being read (or used) will have implications for Data Protection registration. The storage of records may be useful for self-diagnostic purposes and in order that banks can ensure that they maintain a quality service when dealing with Internet customers. Both the 1984 and 1998 Acts stipulate that data must be processed fairly and lawfully[31], as a general rule this means if data uploaded from a web-site is to be put to commercial use the data subject must consent[32] to such use. An example of such commercial use in the banking sphere could be where a customer's data is used to decide on financial services that might benefit them in particular.

The 1998 Act imposes an obligation on the person controlling the data to ensure it is kept up to date and accurate[33] – this obligation is brought forward from the 1984 Data Protection Act. The 1998 Act introduces a new requirement;[34] that "appropriate technical and organisational measures" must be taken to protect the data from unauthorised or unlawful processing and to protect against accidental loss or destruction or damage. What this actually means in relation to banks and Internet transactions could be the subject of some debate. The 7th and 8th Data Protection principles stipulate that the system must posses an "appropriate level of security" and an "adequate level of protection". Given the financial importance of the information that bank's process, the measures would have to be fairly extensive. Measures such as comprehensive risk assessment procedures, (identifying danger from internal and external sources), and thorough testing of all components should avoid any challenge under the principles of the 1998 Act.

Ultimately the consumer benefits a great deal from the two Data Protection Acts. In addition to processing customer data fairly and lawfully, new provisions from the 1998 Act also force banks to be careful that their Internet banking systems are structured so as to posses sufficient security and protection features. Although banks should take this action irrespective of the legislation, the Data Protection Acts do make such action compulsory. The new act also applies a number of new additional provisions for data being transferred out-with Europe, and also for 'sensitive'[35] data, but further discussion is unnecessary here.

---

[29] UK Data controllers, defined (s.1 – 1998 Act)
[30] European Data Protection Directive (97/66/EC).
[31] (1st Data Protection principle. (Sch.1, Part.1 – 1998 Act)).
[32] (*Consent* is a crucial part of the 1st principle - noted in Sch.2 – 1998 Act).
[33] (4th Data Protection principle. (Sch.1, Part 1 – 1998 Act)).
[34] (7th Data Protection principle. (Sch. 1, Part.1 - 1998 Act)).
[35] (Defined - s.2. consequences of processing – Sch. 3 (1998 Act)).

- Financial Service Regulations

Banks, in general, if they have a high level of Internet presence will want to maximise their profitability through the provision of a range of financial services. Additionally, given that the Financial Services Authority (FSA) has recently been given the task of supervising banks[36] as well as the provision of financial services on the Internet, it is important to look at how the financial services' regulations operate in relation to Internet banking.

Banks are regulated primarily by the Banking Act 1987, yet given the breadth of different services which banks now provide their services can often come within the scope of the Financial Services Act 1986. The 1986 Act provides that "Investment business in the UK"[37] must only be completed by those who are duly authorised by a recognised Financial Services regulator. While there is no mention of the Internet within the 1986 Act, the net does provide an ideal forum for the *marketing* of financial services; an activity which is rigorously controlled by the 1986 Act[38]. The 1986 Act is complex and there is no need to go into its provisions in detail, yet it could have Internet Banking implications with regard to advertising, disclaimers, record keeping, penalties and enforcement proceedings. Banks and financial service providers must be aware of its provisions, before the replacement Financial Services and Markets Bill enters into force.

Although current regulatory organisations have not really taken a proactive role in regulating the net, they recognise the need for flexible rules and have intervened in the case of extensive disclaimers. Disclaimers are present in many Web-sites and E-mail communications in order that banks can avoid liability under certain circumstances. However, the use of such disclaimers can be abused. IMRO[39] has intervened when a disclaimer sought to remove fundamental consumer rights. IMRO gave an example of a disclaimer that would, in their opinion, warrant intervention: "[The firm] accepts **no** liability for **any** loss, damage or injury arising as a consequence of any party relying on the content of this web-site".

Those providing services on the net cannot therefore elect to avoid rules; if disclaimers attempt to remove the consumer's fundamental rights regulators *will* intervene. The roles of financial services regulatory bodies are soon to be taken on by the FSA, which already has taken over the supervisory role of the Bank of England. The goal of the government is that the FSA will effectively regulate Internet financial services – whether this will be the case in practice remains to be seen.

- Banking legislation

Bank regulation is a complex mixture of statutes and more informal rules; many current statutes are derived directly from provisions which are more than 100 years old. Banks in the UK are regulated by the Banking Act 1987, which has been altered to an extent by the Bank of England Act 1998 – which switched the supervisory role from the Bank of England to the FSA[40]. An important consideration for newer Internet banks is that this legislation provides that no person may operate a deposit taking business without being authorised to do so.[41]

A key requirement[42] of the Banking Act is that Banks conduct their business in a "prudent" manner. The use of the Internet is a means of conducting business, and hence the structuring of operations over the net, (in particular conducting *transactions*), should be subject to this requirement. Entering into operations before ensuring that their Internet banking system is secure would run contrary to the requirement that banks conduct their business in a prudent manner. Again, provided that banks properly investigate the risks involved and that they test their systems' resistance to attack, and its likelihood of crashing then the "prudent manner" requirement will be met. However, this 'prudent' requirement should always be noted, because it could offer consumers a route to a liability action.

---

[36] Bank of England Act 1998 - switched supervisory role from Bank of England to the FSA.
[37] S.3 – Financial Services Act 1986.
[38] S.57 – Financial Services Act 1986.
[39] (Investment Management Regulatory Organisation), Source: Nola Beirne, Andrew Herring, *Financial Services regulation and the Internet in the UK*, (The Company Lawyer vol. 19 No 9, 1998).
[40] For details see Part III - Bank of England Act 1998.
[41] Banking Act 1987, s.3.
[42] Banking Act 1987, s. 11(1)(a) and par. 4 – Sch.3.

As part of the requirement to operate in a 'prudent manner', banks are required to maintain accounts and other records and also adequate systems of control. Provision will have to be made, therefore, for a system which records Internet transactions in a suitable form – whether by paper records or in the form of other electronic back-up systems. This requirement forces banks to consider carefully the best system architecture, which allows them to stay within the parameters of operating in a prudent manner.

Effective regulation and the imposition of conditions on bank operations, (at the moment through the Banking Act 1987) will benefit the consumer. Although banking regulation is often referred to as being heavy, it does *not* appear to be stopping new, smaller banks from entering the Internet banking arena. No guidance has yet been provided to banks as to how the Banking Act might operate in relation to Internet services. Banks will have to exercise sound judgement in considering how the regulations are applicable to Internet services. The consumer should be able to benefit from the Banking Act's restrictions.

- Consumer Credit legislation

Bank operations often fall within the realms of consumer protection legislation, in particular the Consumer Credit Act 1974. This statute, even more than the Banking Act, was written with paper records[43] very much in mind. The DTI have stated[44] that consumer credit protections should apply equally to traditional and electronically formed agreements. This is merely guidance, (not legal certainty), but perhaps it is also a good indication of the approach the courts would take if an Internet banking customer sought redress under the 1974 Act. Banks should therefore ensure that their Internet provisions comply. The fact that Financial Services Regulators generally provide that the terms of the Consumer Credit Act **must** be obeyed, (in order to remain a member of that body), negates the question of the *strict* applicability of the Act. Additionally, obeying or complying with the Act would enhance consumer confidence, and might go someway to convincing new customers that Internet transactions are as safe as paper transactions. Until new legislation or, alternatively, a ruling is made to the contrary the Consumer Credit Act will continue to have a major impact on how Banks and other Financial Service providers operate on the Internet.

Future regulatory measures

- Is Internet regulation necessary?

The nature of the Internet provides sizeable challenges to lawmakers throughout the world. Generally, there is a lot of debate about whether regulation is actually necessary and if so what the best way is to approach the legislation. The conclusion emerging from debates appears to be that legislation *is* needed, but it should promote the growth of the net and encourage commerce; for both traders (or banks) and consumers it should be a safer place to transact. New legislation should allow flexibility – so that courts will be able to interpret the legislation in line with emerging new technologies.

The next problem for investigation is how to deal with the regulation of such a complex and rapidly changing forum. Experts were quick to recognise that uncoordinated action through domestic statutes would not be suitable. Firstly, statutes generally take too long to come into force, given that technology changes so rapidly. Despite statutes being important to provide a background of hard law (a framework from which to move forward), self-regulation and other soft law can be equally, if not more important. Secondly, to avoid conflicts between national laws, co-ordinated multinational action is needed. On a multinational level, the United Nations Commission of International Trade Law (UNCITRAL) created a model law[45] to remove legal barriers to electronic commerce. The European Commission created and proposed a number of key directives– the Data Protection Directive,[46] (which in the UK led to the Data Protection Act 1998), and the draft directives on Electronic Commerce[47] and

[43] Credit Agreements must be documented in the prescribed form and signed in the prescribed form – s.61 Consumer Credit Act 1974.
[44] DTI, *Net Benefits: the electronic commerce agenda for the UK*, (October 1998).
[45] UNCITRAL model law on electronic commerce, December 1996.
[46] Dir 97/66/EC.
[47] Com(98) 586 final, 18/11/98.

Signatures[48] and on Distance Marketing of Financial Services[49]. On a national level, the UK government has been relatively quick to recognise the value of electronic commerce. The Electronic Communications Bill, in part a reaction to legislation emerging from Europe and currently in draft form, is designed to meet the governments objective of making the UK the "best environment for electronic trading" by 2002. This paper shall examine these measures in turn, looking in particular at how they tackle some of the risks of Internet banking, and what they provide for the On-line banking consumer.

- UNCITRAL model law

The UN recognised that differing rules on electronic commerce between countries could create partitioning of the market, and hence decided to create a "model" law. The UNCITRAL model law[50] is not binding, but if it's provisions are adopted, electronic communications are given the same legal effect as paper based communications. As will be seen this 'equivalency' approach is a popular theme with proposed electronic communications laws. Presently, the UK is only taking a limited equivalency approach in its proposed Electronic Communications Bill. The bill contains a mechanism whereby ministers may amend legislation which creates a barrier to electronic formation of contracts. The approach is driven by the lack of time to consult and formulate a more unique – "Internet focused" approach. UNCITRAL did not create new law; the "model" law merely seeks to adapt existing law to apply it to electronic communications. If the UK were to amend its legislation containing requirements that contracts are in "paper" form, then more banking services could be completed on-line. The model law was adopted by the UN in December 1996 and hence was really just a first attempt at a form of Internet regulation.

- Proposed European Measures

The European Union gave the Commission the (impossible) task of creating a coherent European legal framework for electronic commerce by the year 2000. The commission were hence quick to take action, recognising the potential for inter and intra- European trade which electronic commerce allows. The proposed Electronic Commerce Directive covers most on-line services (hence Internet banking is included), the wide definition being: "services provided at a distance[51] by electronic means, and at the request of a recipient". The initial provisions concern service providers established within a territory being subjected to the national laws of that territory. The directive then moves on to give protections to providers of electronic commerce and their consumers, (i.e. Internet banks and their customers). To reduce anonymity associated with the net – the European provisions allow the customer to identify and contact the service provider. Very professional looking "fake" web-sites can be easily created allowing fraudsters to convince Internet consumers to part with their money[52]. However, article 5 provides that the following must be available to the user of a web-site: the name and address of the service provider, a method of instant contact, trade mark information and any authorisation scheme covering the provider. By making this information available the customer would be in a better position to know whether the service is from a reputable source.

The proposed directive, like most legislation in this area, seeks to give the same effect to contracts concluded by electronic and conventional means. Section 3 of the proposed Electronic Commerce directive deals with the formation of electronic contracts. Within section 3, article 9 seeks to ensure that member state legislation does not deprive electronically formed contracts of legal effect. The Consumer Credit Act 1974 and the Money Laundering Regulations 1993 would perhaps fall into such a category. Article 10 provides that the service provider (in this case the bank), must set out clearly how the contract will be concluded, e.g. by e-mail or clicking an icon. This would go someway to alleviating fears of "accidental contract formation", which could be a concern to bank customers.

---

[48] Com(98) 297 final, 13/5/98.
[49] (Modified) Com(99) 385, 23/07/1999.
[50] For text see (www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm).
[51] Note: this does not necessarily mean 'cross-border', therefore the UK located bank and customer communicating at a distance would fall within the definition.
[52] The Bank of England issued warnings about fraudsters holding themselves out to be Internet banks. (Source: Financial Times on Sunday, Jan 2000).

The proposed directive also clarifies the issue of the moment at which the contract is concluded.[53] The directive, if implemented, will add a welcome dimension of certainty to electronic contract formation. By taking a common approach to contract formation, member states would ensure that consumers only enter agreements by giving their full and informed consent. Such certainty would assist the development of Internet banking.

Another proposed directive, this time on a framework for digital signatures, was given its first reading in January 1999 and is designed to supplement the aforementioned Electronic commerce directive. The directive provides that Digital signatures should have the same legal effect as hand-written signatures. This would enable banks to conclusively identify the other party to a contract. This raises interesting issues, such as whether (and if so how) the directive could change money laundering procedures.

The Distance Marketing of Financial Services is of could be of particular importance to the Internet Banking consumer. The directive is to supplement the existing Distance Selling directive[54]. Importantly, the directive covers any banking, insurance, investment or payment service concluded between an information society services provider (e.g. the bank) and an individual consumer by means of electronic communications (e.g. the Internet). The consumer, who may make *exclusive* use[55] of electronic communications up to (and including) the time when the contract is actually concluded, receives new protections. The bank must render accessible, in a direct and permanent manner, a comprehensive set of details[56] prior to the contract being concluded. This information includes,: the main facets of the banking service, the price and payment arrangements, the length of the provision of the service along-with any right of withdrawal, information on cancellation of the service, the governing law (*if* customer and bank are located in different territories) and any out-of-court procedures for re-dress. Additionally, once the contract has been formed (on-line), the terms and conditions must be communicated in writing or another durable medium, in a "clear and comprehensible" manner. "Another durable medium" can be a floppy disk or e-mail[57], therefore paper records are not made an essential feature of Internet financial services. A general right of withdrawal exists for a period of 14 to 30 days[58] after the contract is formed. Again, the risk of "accidental contract formation" is addressed – the directive stating that silence can*not* constitute agreement[59]. Despite its name, the Distance Marketing of Financial Services directive *does* apply to relationships where service provider and customer (or bank and consumer) are located in the same jurisdiction.

The above European directives, if implemented, should ensure that the consumer gives his full and informed consent to banking contracts. They do not specifically deal with post-contractual problems, but the directives should ensure that a common approach is taken to consumer protection – which in turn should facilitate Internet banking. The uncertainty surrounding legal rights and the status of electronic transactions and contracts is certainly a barrier to some against entering the Internet Banking arena. To ensure this problem is eliminated and the directives, when implemented, are effectual – then consumers must be made aware of the existence of these new rights and protections.

- Proposed UK Electronic Communications Bill

The UK Electronic Communications Bill was a direct result of the governments wish to make the UK more competitive in the "virtual" marketplace. Equivalency between digital and hand-written signatures is a key aim of the bill, the UK adopting a similar approach to that advocated in the proposed Digital Signatures directive. Legal recognition of electronic documents is another aim of the bill. The bill is to come into force relatively quickly – the DTI are pushing to move forward deadlines, requiring a quick investigation into the legislative changes required in English and Scots Law.

The bill could have important repercussions for Internet banking. It is possible that more services could be based solely on-line. As an example, on-line loans could possibly be granted over the

[53] Article 11.
[54] Distance Selling dir. (97/7/EC), protected the consumer but did not include financial services, (Article 3).
[55] Article 2.
[56] Article 5.
[57] Article 2.
[58] Article 4.
[59] Article 9.

net – the money appearing automatically in the customer's account. Digital signature recognition would avoid the need to print out, sign and post in a document, speeding up the loan application process considerably.

Legal recognition of electronic documents would benefit both banks and their customers, removing a lot of the uncertainty that surrounded electronic contract formation. It is hoped that the eventual legislation will make the interpretation of existing legislation, (such as the Consumer Credit Act and the Unfair Contract Terms act), a lot clearer in relation to electronic formation of contracts.

There are, however, some criticisms directed towards the bill. The way in which equivalency is to be achieved is through amendment of existing legislation which makes writing (in some form) an essential part of valid contract formation. Such amendment must be accompanied by instructions on how the legislation will deal with electronic contracts. Amending existing law does not appear to facilitate the creation of a legal framework for E-commerce. This process also appears time-consuming, although it would eliminate barriers to E-commerce and hence Internet banking.

A recent article[60] highlighted the government's concentration on encryption as a major drawback. The bill, it is suggested, seeks to do too much – concerning itself with the negative aspects of encryption. Part III deals extensively which encryption, but widespread criticism is likely to see the section removed before the bill becomes law.

The British Bankers Association (BBA) has reacted very positively[61] to the proposed bill. The BBA welcomed the government's intention that the law should not discriminate between traditional and electronic means of doing business. The BBA also recognised the importance of the legal recognition of digital signatures, stating that it would help the market grow and would hence improve consumer choice. "Flexibility" was seen as a key issue, and the BBA, like many other e-businesses were pleased to see that the government drafted legislation to remain "technology neutral" – given the rapid development of technology in this area. The BBA director offered general support for the Electronic Commerce Bill stating,: "New channels of banking offer greater choice for customers, and banks believe that this new legislation, if sensitively drafted, could help to ensure that these new channels thrive".

Conclusion

- *New competition in Banking*

Internet banking offers banks considerable cost savings on a number of levels in comparison with normal banking methods. Net banking also offers a forum to advertise a wide range of lucrative services. Bank customers can shop around different web-sites for the most competitive services and interest rates. With new banks offering ultra competitive Net services, the older banks are experiencing competition like never before. A lot of banks are being forced into having an advanced Internet presence merely to maintain their existing client base. This new culture of competition appears, on the face of it, to be good news for consumers. Yet concerns about the compatibility of the Internet and banking are creating a barrier, stopping many consumers from taking advantage of this new, competitive market.

- *Internet & Banking Incompatibilities*

The first "incompatibility" to be looked at is the structure of the Internet and the financial value of the customer information travelling on it. Only serious cases of "hacking" (or web-site attacks) tend to be publicised, yet the general consensus seems to be that a lot of attacks are either being covered up, or are going unnoticed. The teething problems[62] that newer banks have been experiencing provide ideal examples of weak links that could be exploited.

The second major "incompatibility" seems to be Internet banking and legislation. The Consumer Credit and Money Laundering provisions would certainly fall within the categories of

---

[60] Andrew Lothian, *E-commerce: de-bugging legacy legislation*, (Scots Law Journal, October 1999).
[61] BBA, *Banks welcome Government E-commerce plans*, (5 March 1999).
BBA, *Banks now demand appointment of e-envoy*, (23 July 1999).
[62] *Egg* – credit card details were made openly available, *First-e* – deposits were not correctly credited to customer accounts.

measures "stifling the growth of E-commerce" which the EU wish to eliminate. With no guidance on the point, banks are observing old legislation drafted very much with "paper" records in mind, while being uncertain as to its applicability.

It is undeniable that while the Internet is in many ways ideal for the provision of banking services, no suitable framework yet exists to protect consumers. The development of Internet banking is progressing at lightning speed. As previously discussed, banks are forced to defend their status in the retail banking sector against new competitors. If banks do *not* offer advanced cyberbanking they stand to lose out, yet without proper testing the risk is a flawed system would be created and bank reputations could be on the line. For banks the task of creating an Internet service has to be combined with risk management procedures. While this paper has sought to reach a conclusion on the *consumer* risks of banking on the net, an examination of difficulties banks experience has been unavoidable. At present the consumer must also take on a risk management role. While we can look at how existing legislation might assist the consumer and can predict how such legislation might be interpreted with regard to Internet banks, we cannot say with any certainty that all the legislation is applicable.

- *Legislation*

Legislation has rarely been able to cope with the fast pace at which technology changes, yet a common approach by banks to the existing legislation would at least give the consumer some confidence that a standard of security would be maintained when dealing with their data. Looking at existing legislation we can see some important protections, but only the newly drafted 1998 Data Protection legislation can be said to have considered the commercial use of the Internet.

The main objective of the Data Protection Acts is that data is processed fairly and lawfully. Banks, while they will already by registered under the 1984 Act, will have to ensure that the terms of their registration include uploading personal information from their web-site. In the main the data protection principles ensure that banks do not put personal data to unauthorised use and that the data is accurate. The new 1998 Data Protection Act adds to the principles that appropriate technical and organisational measures must be taken to protect the data. Although little guidance is given as to the meaning of these new principles, it is likely that the financial value of the data processed would necessitate a high level of security measures to gain the approval of the data protection registrar.

Financial service regulation is currently going through a period of change, the FSA acquiring the supervisory role of all the previous financial service regulators. Already the FSA has taken over the Bank of England's supervisory role and the government has also given the FSA the task of regulating financial services on the Internet. The Internet provides the ideal forum for banks to market the type of services falling under the control of the Financial Services Act 1986, (which will soon become the Financial Services and Markets Bill). Consumers should be able to take some comfort that banks must be authorised under the 1986 Act, and hence they should be able to derive some protection from financial service regulations, ensuring "investor protection".

1986 Act authorisation, in other words membership of a regulatory body, is often conditional on the compliance with the Consumer Credit Act 1974. Again some comfort should be derived from this, as offering loans on-line should not allow banks to escape the, somewhat onerous, credit agreement requirements. The DTI also recently published an agenda[63] that included electronic commerce consumer protection measures. The agenda specifically stated that electronic commerce transactions are subject to the traditional rules on consumer credit. Although not a legal certainty, this suggests that the Internet banking consumer could seek redress under the 1974 act should things go wrong.

Looking at the Banking Act 1987 reveals a number of restrictions on how banks should conduct their business, not least of which is the requirement that banks conduct business in a prudent manner. How these restrictions are to work in relation to Internet operations is unclear. Whilst the act could be adapted to apply to Internet banking, no guidance has yet been given as to how this might be achieved.

In the absence of guidance to the contrary, banks are trying to observe the terms of banking

[63] DTI, *Net Benefits: the electronic commerce agenda for the UK*, (October 1998).

legislation in operating their Internet services. The current situation is unsatisfactory, only the provisions of the Data Protection Acts are *definitely* applicable to the Internet consumer. Both banks and consumers run the risk of finding that agreements and transactions made on the Internet are unenforceable, or do not have the same legal status as those formed in a more traditional manner. The multitude of different "Internet-focused" legislative provisions currently making there way through the various stages towards enactment reflects the unsuitability of ageing legislation to deal with the new transactions which the Internet allows.

- *Future protection measures*

Reviewing the provisions of the proposed Electronic Commerce and Distance Marketing of Financial Services directives shows a desire to achieve a common European approach to the provision of a high level of consumer protection in E-commerce operations. Underlying the technicalities of these directives is a need firstly to eliminate those domestic measures[64] restricting E-commerce followed by the creation of a system of Internet contract formation which ensures that parties give their full and informed consent. Provided that consumers were made aware of the protections afforded by these directives (reflected in national legislation), then 'optimum protection' could be achieved in the field of Internet banking. However, there may be some difficulties in bringing the directives into force. The difficulty of gaining member state agreement has proved an insurmountable barrier to far less controversial matters in the past. Even if agreement was achieved, technology is likely to have moved forward quite dramatically before these directives became enforced.

The UK Electronic Commerce Bill, which was warmly received by the BBA, could make some important changes as regards Internet Banking. Part II of the bill makes provisions for the facilitation of E-commerce, (Internet banking falls under such a heading). These provisions provide ministers with a power to amend legislation which requires writing, (or the maintenance of paper records), and therefore acts as a barrier to electronic contract formation. The operation of this power is conditional on the provision of a precise electronic alternative to the original procedures. Enacting such modifications, although very much a step in the right direction, is likely to be a slow process. Another drawback is that the Bill makes no mention of the creation of *new* consumer protection provisions, such as those suggested by the European Commission. If the government wishes to facilitate Internet banking, then it will have to take more positive action.

Ultimately using the Internet for banking will never be free from danger. New hard (statute) law is required in terms of consumer protection. The additional protections suggested by the proposed European directives seem ideal for this purpose. Although difficulty may be experienced in amending their provisions to make them acceptable to member states, ultimately the consumer needs the protections which they can offer.

Comparing the *snail's pace* with which legislation moves through government to the *rapid* changes in banking and computer technology is perhaps illustrative that there will never come a time when the two are on exactly the same wavelength. The quickest way to instil more certainty and greater consumer protection into Internet banking would be through the development of Codes of Practice. For example, perhaps the Code of Good Banking Practice[65] could be amended to incorporate codes of conduct governing Bank operations on the Net. Although not legally binding, (and therefore quicker to enact), such an amendment would be a powerful incentive to maintain at least a minimum standard of consumer protection.

- *Summary: Present Problems/Future Solutions*

As it stands, the consumer protection legislation discussed cannot be relied upon. Customers will have to be aware that banking on the net involves a level of danger not experienced in traditional banking circles. It is up to the consumer to decide whether the improved services on offer justify the risks involved. If consumers decide to take the risk they would be well advised to carefully consider the terms and conditions of the arrangements they enter into. Presently banks guarantee that they will

---

[64] For example: Consumer Credit Act 1974, Money Laundering Regulations 1993.

[65] BBA, *Code of Good Banking Practice*, (2nd ed., 1994)

meet most losses incurred by the customer through their services, yet if problems emerge on a *large* scale it is not unforeseeable that banks could suffer great losses and fold (especially undercapitalised newer banks) – leaving the customer high and dry.

Although the long-term approach taken in the UK seems to be to make electronic and paper based transactions equivalent, the new risks of the Internet also bring the need to supplement existing law with new "Internet-focused" rules. The proposed European provisions, if they find their way into UK law, would drastically improve the Internet banking consumer's safety. An effective combination of existing and new legislation should make the Internet a safer place to transact, but softer forms of law will also have an important role to play. Codes or guidance, although not legally binding, can have sanctions attached and do have the important advantage of being able to be created or changed quickly to match the development of Internet services.

Bibliography-

Reports:

Banking Services: Law and Practice Report by the Review Committee, February 1989, Cm 622.

Encyclopaedias:

1. *Information Technology and Law Encyclopaedia*, Chapter 5 - Electronic Banking and Financial Services, March 1999.

2. *Banking Law Encyclopaedia*, Plastic Cards and Digital Cash, Internet Banking and Digital Cash.

Textbooks:

1. L.D. Crerar, *The Law of Banking in Scotland*, 1996
2. Paget, *Law of Banking*, 11th edition
3. D.B. Caskie, *Wallace and MacNeill's Banking Law*

Articles:

4. Alan Gahtan, *On-line Banking*, (23 May 1997,Internet source).
5. Anon, *Banking Business and technology: "Pointing a finger at the future"*, (CA Magazine, March 1997).
6. Anon, *"Internet Banking" - an overview*, (Journal of Internet Banking and Commerce, 1999).
7. Anon, *Advanced Internet Banking explodes in Europe*, (Press release - 26 Oct 1998).
8. Anon, *UK Digital Banking set to boom*, (Internet article, 22 July 1998).
9. John Naughton, *"Chequered careers"*, (Guardian, 13 June 1998).
10. Jill Treanor, *"Rate of Branch closures slows as customers revolt"*, (Guardian, 1 June 1999).
11. Sean Coughton, *"You can bank on Net gains"*, (Guardian, 17 April 1999).
12. Anon, *"Screening your account"*, (Guardian, 16 June 1999).
13. Nick Collen, *Internet Banking and Web TV*, (anon source).
14. Anon, *Bank of Scotland launch BOSinternet and free PC banking*, www.bankofscotland.co.uk
15. BBA, *Banks demand appointment of E-envoy*, www.bba.org.uk
16. Anon, *Online banking (egg)*, (Financial Times (FT), 19 August 1999).
17. Anon, *Easyjet founder to set up Internet bank*, (FT, 13 August 1999).
18. Anon, *Royal Bank of Scotland to offer loans on-line*, (FT, 16 August 1999).
19. Anon, *Internet only bank launch*, (FT, 29 May 1999).
20. BBA, *Banks welcome government e-commerce plans*, (5 March 1999).
21. Anon, *First active to sell mortgages on the Internet*, (FT, 26 August 1999).
22. Anon, *European on-line banking outstrips US competition*, (FT, 23 August 1999).
23. Anon, *Banks hit 32% rise in counterfeit card fraud*, (FT, 21/22 March 1999).
24. Anon, *Banknet Electronic Banking Service, worlds first*, www.193.118.187.101/help/bank/info
25. Anon, *Royal Bank of Scotland to offer on-line loan approval*, (The Herald, 16 August 1999).
26. *Summary of responses to consultative letter on electronic commerce*, changes to Companies Act 1985, (Company Law and Investigation Directorate - Branch 1, 1998).
27. Anon, *Electronic Commerce, "What does the future hold?"*, (PLC, May 1999).
28. *Banknet - frequently asked questions*, 193.118.187.101/help/bank/info/echeque
29. *Electronic payment instructions- A Guide*, (Anon).
30. *On-line banking report*, www.onlinebankingreport.com
31. *Unisys - Internet banking in Europe*, www.unisys-finance.com
32. *Barclays on-line banking*, www.personal.barclays.co.uk
33. *On-line Banking Report* - True World Internet Banks
34. *On-line Banking Report*, www.netbanker.com
35. *Bankweb:International Bank, Great Britain*, www.bankweb.com
36. Chris Reed, *JACK Report*, (Computer Law and Practice (C.L. & P.), Jan/Feb 1990).
37. Heather Rowe, *Legal issues between banks sharing networks*, ((C.L. & P.), Sept/Oct 1990).
38. Ranald Robertson, *Limitation of liability in EFT transactions*, ((C.L. & P.) Sept/Oct 1990).

39. Alex Sheshunoff, *"Wait is over forInternet banking"*, (ABA Banking Journal (ABA), June 1999).
40. *"At last Internet banking takes off"*, (ABA, July 1999).
41. Sanjev Warna-Kula-Suriya, John Croswait and Tim Parker, *Conquering Global Markets, financial services and the Internet*, (PLC, August 1999).
42. Wayne L. Rhodes, *"Each new technology sets security back"*, (AS/400 system management, August 1998).
43. KPMG, *Internet gateways can leave the door open for fraudsters*, (Management Accounting, January 1999).
44. Mike Plonien, *Electronic commerce on the Internet*, (The CPA Journal, May 1998).
45. *Natwest tests out TV banking*, (Marketing journal, Jan 28 1999).
46. Donald Jay Korn, *The ABC's of Banking On-Line*, (March 1996).
47. Anon, *BASIC PAYMENT INSTRUMENTS*, (1992).
48. Anon, *Natwest Bank surges into cyberspace*, (July 1996).
49. Anon, *Electronic Banking to grow more than 30% - 2005*, (October 1998).
50. Jaqueline Day, *Electronic Wallet technology*, (January 1995).
51. Anon, *HOBS - PC is key to middle market*, (Jan 1991).
52. Anon, *Money on the line*, (November 1995).
53. Anon, *Moniker Magic*, (September 1994).
54. Anon, *Promising electronic money*, (May 1995).
55. David Jones, *Payment systems: UK now second*, (March 1993).
56. Kevin Hart, *Direct access to automated payments*, (1994).
57. Richard Allen, *APACS - payments systems in the 1990's*, (Jan 1990).
58. Anon, *Tech Survey: Irresistable March of Switch*, (November 1991).
59. Jim Balderston, *On-Line cash: a penny for your thoughts*, (July 1996).
60. Joseph LaPagilia, *Moving money down the wire (US)*, (August 1996).
61. Mark Lewis, *Internet Banking - 200 legal systems*, (PLC, August 1999).
62. Ian Darby, *Banks face up to on-line challengers*, (March 1999).
63. Anon, *RB of S to pioneer on-line banking*, (January 1997).
64. David Summer Smith, *Wiring your accounts*, (February 1998).
65. Anon, *Staying on an even keel (Moody)*, (February 1998).
66. Anon, *Barclays scraps screen trials to push net system*, (June 1999).
67. Anon, *RB of S melds internet and phone bank*, (February 1997).
68. Anon, *Consumers at home with PC Banking*, (November 1996).
69. Anon, *Co-op offers TV banking on Sky intertext system*, (July 1996).
70. Anon, *Banks ramp up e-purse trials*, (April 1996).
71. Anon, *Banks launch Global Mass Funds Transfer (SWIFT)*, (November 1992).
72. Christopher Stoakes, *Litany of rules that lag on-line banking*, (PLC, Aug 1999).
73. Anon, *Banks look to Net gains*, (The Herald, 23 October 1999).
74. Andrew Kinnes, *Internet Banking*, (Shepherd & Wedderburn Business briefing bulletin, August 1999).
75. Heather Rowe, *E-commerce Policy developments in the UK and the EU*, (SCL magazine, June/July 1999).
76. Iain G Mitchell, *Future Regulation of E-commerce and Commercial Communications in the EU*, (SCL magazine, June/July 1999).
77. Anon, *Risks Associated with E-cash*, (Internet source, 1998).
78. Steve Bell, *First Direct faces up to rivals*, (Marketing, November 1998).
79. Adam L Penenberg, *Microsoft and Intuit in E- Bank Détente*, (January 1997).
80. Anon, *OnLine Banking:UK users could leap to 7 million*, (Haymarket Publishing, March 1999).
81. Alex Plavsic, Tad Dippel, Shabir Hussain, *IT Facilitating Fraud*, (International Review of Law, Computers and Technology, August 1999).
82. Nola Beirne, Andrew Herring, *Financial Services regulation and the Internet in the UK*, (The Company Lawyer vol. 19 No 9, 1998).
83. Andrew Murray, Douglas Virk and Scott Wortley, *Regulating Electronic Commerce*, (International Review of Law, Computers and Technology , August 1999).
84. Lars Davies, *Contract Formation on the Internet: Shattering a few myths*, (Law and the Internet – Regulating Cyberspace, 1998).

85. Andrew Lothian, *E-Commerce: de-bugging legacy legislation*, (Scots Law Gazette, October 1999).
86. Jonathan Duffy, *UK Personal Account (Part 1) - Getting Started*, (BBC News On-line, November 1999).
87. Anon, *Money Program: Investigation into Internet fraud*, (BBC News On-line)
88. Anon, *Virtual Legality*, (CA Business Banking, January 2000).
89. Ruth Sunderland, *Big Four threatened by new breed of bank*, (Financial Mail on Sunday, January 2000).
90. Alison White, *On-Line Banking*, (The Scotsman, July 1999).
91. Anon, *Harper Macleod IP & T Briefing*, (August 1999).
92. Anon, *Harper Macleod E-Commerce Bulletin*, (August 1999).

Legislation:

93. Data Protection Act 1984.
94. Data Protection Act 1998.
95. Financial Services Act 1986.
96. Banking Act 1987.
97. Consumer Credit Act 1974.
98. Unfair Contract Terms Act 1977.

Other Documents:

99. Proposal for E-Commerce directive, COM(98) 586 final.
100. Proposal for Distance Marketing of Financial Services, COM(98) 468.
101. DTI, *Building Confidence in Electronic Commerce – Consultation Document*, (June 1999).
102. DTI, *Secure Electronic Commerce Statement*, (April 1998).
103. DTI, *Promoting Electronic Commerce*, (July 1999).
104. DTI, *Net Benefit: the electronic commerce agenda for the UK*, (October 1998).