

INTERNATIONAL SOCIETY FOR THE REFORM OF CRIMINAL  
LAW  
16TH INTERNATIONAL CONFERENCE

Technology, and its Effects on Criminal  
Responsibility, Security and Criminal Justice

Charleston, South Carolina Dec. 6 - 10, 2002

**Rosalind Wright**  
**Director,**  
**The Serious Fraud Office**  
**London**

**Cybercrime from a UK perspective:  
The problem and some solutions**

There has been enormous growth in the use of the Internet. By May 2001, the last figures we have to hand, 10 million homes in the UK were connected to the Internet. This is up from a figure of 6 million in 2000. A survey last year found that approximately 33 million people in the UK now use the Internet. Ever more people are routinely using technology in their daily lives and the range of information technology products available to them is increasing.

The use of cyberspace for commercial trading represents a colossal opportunity to enhance and cheapen the flow of information, goods and services.

This growth is to be welcomed. *e-commerce* is the way of the future and making it a safe and user-friendly way of conducting business, taking advantage of the opportunities of the information society must be the way forward. The essential features of what some call cyberspace are the speed with which huge quantities of information can be transmitted, the fact that it ignores borders, the remoteness of action from consequence and the anonymity offered by the procedures.

It is not just the good guys who see the attractions of such technology; users include criminals and so we must ensure that investigators and prosecutors in the SFO and the CPS are able to investigate and prosecute those who commit what I may loosely call cybercrime.

The word cybercrime conjures up the 1960's sci-fi image of androids committing new unheard of offences with ray guns. Fortunately, so far cybercrime has turned out to be

nothing so unearthly but it is an extraordinary new threat. The highest industry estimate I have seen is that global cybercrime cost 40 billion US dollars in 2001.

It is my view, which I share with others, that out of the ordinary new techniques and skills are required to deal with it.

Concern has regularly been expressed that technology now available to criminals is such that fraud and other related crime may be too easy to commit, or that, even where detected, the present procedures may be too cumbersome to enable effective investigation and prosecution.

Most crime involving computer technology is simply criminals using computer technology, in a fairly complicated fashion to achieve their aims. The Internet has increased the opportunity for fraudsters to rip people off by inviting them to send money for non-existent goods or services to create false share markets in a variety of ways, commit spectacular banking frauds and in the case of pornographers has made it possible to deal with incredible numbers of images and relay them round the world or gather them from around the world at exotic speed.

Of course there are also the new crimes of computer misuse – hacking, disseminating viruses and planting logic bombs - are crimes would not have existed without computers.

Investigators were faced with a number of pressing questions in the mid-1990's.

- How do they cope with the international nature of fraudulent activity where the Internet creates a facility to ignore boundaries?
- How can their powers be expanded to gain access to, or after the crime or to intercept during a crime material that is communicated electronically and is often encrypted.
- How can evidence best be presented in court in a way that is understandable, reliable and admissible?

*We hope we've found most of the answers*

### **The criminal jurisdiction**

The criminal jurisdiction to deal with cybercrime is now very wide – the relevant provisions are Part I of the Criminal Justice Act 1993, the Criminal Justice (Terrorism and Conspiracy) Act 1998 and the Computer Misuse Act 1990. By and large if you commit an act in the UK, which takes effect outside the UK, or an act outside the UK, which takes effect in the UK, there is jurisdiction to try you in the UK.

### **Investigating**

The Regulation of Investigatory Powers Act 2000 provides for the interception of traffic on the Internet and access to stored data.

The Bramley provisions in Part II of the Court and Police Services Act 2000, which are soon to be brought into force, consolidate the piecemeal statutory reforms, which sought to deal with the special problems arising from the seizure of computers or the imaging (copying) of electronic data and examination elsewhere whilst preserving the forensic integrity of the seized or imaged material.

*Making such evidence more easily admissible at trial.*

Here prosecutors and judges give thanks for the repeal of section 69 of the Police and Criminal Evidence Act 1984 in the Youth Justice and Criminal Evidence Act 1999.

Section 69 PACE commenced life as an enabling provision - to enable computer evidence to be more readily receivable in evidence at trial by means of a certificate "that the computer was operating properly at all relevant times" - but by the mid 1990's this provision had turned into a hurdle as so many computers was involved in a single transaction e.g. a withdrawal from a cashpoint in Paris of 2000 Francs from your English account.

I should also mention here the major developments in the use of technology used by the Serious Fraud Office and CPS to capture documents in digital form and present them to court in the paperless format.

### **Prosecutors**

From a prosecutor's perspective cybercrime often requires an understanding of complex technical issues. The knowledge and expertise in these areas is predominantly within the industry and specialised police units. Therefore, effective partnership working is essential to ensure that cases are properly prepared for trial.

The benefits of such an approach were apparent in the much publicised "w0nderland" [sic] case which came to trial a year ago at Blackfriars Crown Court. This was the successful prosecution of a large-scale international paedophile ring (120 suspects in 13 countries – 10 suspects were in the UK). The ring used a secure Internet channel to exchange obscene pictures of children. 750,000 such images were seized in the UK. Prior to involvement in this case, the senior lawyer responsible for the prosecution had, understandably and surely forgivably, only limited knowledge of cybercrime issues. However close liaison with the police and experts allowed her to grasp the technical issues quickly, review the case effectively and advise on how the evidence should be presented to the jury.

The SFO have had our own in-house computer forensic unit for many years. They are familiar with seizure, imaging and the examination of the electronic data in relation to frauds. The case of Chiragh, a prosecution arising from BCCI, was an example where hidden material was found, decrypted, reconstructed and the SFO were able to prove who had created or altered the documents using the context information i.e. the sequence the data was laid onto a disk and the dates and times that happened.

In a recent case in relation to a request from Jersey in relation to offences in the financial sector in Jersey the SFO executed four search warrants and seized or imaged material from computers at four premises. The task was routine for the SFO, what was notable was that it was an incoming request for mutual legal assistance.

This brings me to co-operation.

### **Domestic co-operation**

The recognition of the need for effective domestic partnership working in this unique area led to the setting up of the Internet Crime Forum. This is a multi-agency forum with representatives from industry, law enforcement and prosecution authorities. The CPS has been a member of the Internet Crime Forum since its inception in 1997 and has benefited from the contacts it has made. One simple example of this was a conference on computer crime organised for CPS prosecutors in 1999. The speakers were predominantly members of the Internet Crime Forum who were keen to share their expertise with prosecutors.

The Forum has also given law enforcement agencies a much greater understanding of the industries capabilities and resource implications in relation to gathering and preserving evidence from the Internet. Industry representatives have also welcomed the opportunity to develop a greater appreciation of the legal requirements of gathering and preserving evidence.

In April 2001 the National High Tech Crime Unit was set up to provide advice, support and training to local police forces and to investigate the most serious cases. The CPS has established good links with this unit and works closely with its officers to ensure the quality of advice the CPS provides will reflect the standards that were set in the Wonderland case.

### **International co-operation**

The Internet Crime Forum model for partnership working has been a success and has influenced thinking at an international level. Some of you may know that the Council of Europe's Committee of experts on cyberspace has drawn up a Convention of Cybercrime. The Convention was opened for signature on the 23 November 2001 and signed by the UK on that date. The Convention is intended to provide a common criminal policy amongst aimed at the protection of society against cybercrime. It will require the 41 contracting states to adopt appropriate legislation and to provide arrangements for fast and reliable international co-operation. As one might expect in a document from the Council of Europe it will always ensure that a proper balance is maintained between the interests of law enforcement and respect for fundamental human rights. The Cybercrime Convention should ensure there is effective international co-operation in such cases and also that there are no loopholes within contracting parties' legislation that would allow such criminality to go unpunished. UK legislation may needed in some areas, in particular Article 16 and 24 require the expedited preservation of data at the outset of an investigation. This is considered by all law enforcement and security and other agencies as being an essential tool to combat cybercrime where evidence can be altered or deleted at the touch of a button by a suspect.

**Looking beyond Europe now** - the G8 High Tech Crime Sub-Group (of the G8 Organised Crime Group) has organised a number of meetings between industry and law enforcement agencies to discuss issues of mutual interest. The CPS is part of the UK delegation of the High Tech Crime Sub Group and attended the last joint meeting with industry, which took place in Tokyo last year under the Japanese Presidency.

Issues discussed included those arising in the Cybercrime Convention - data preservation, data retention and the training of investigators and prosecutors. Dialogue at an international level is vital as the Internet is a global communications network, which does not recognise jurisdictional boundaries. Therefore, assessing how we can improve mutual legal assistance whilst recognising the sovereignty of individual countries is a difficult but important challenge that needs to be faced. The work in the G8 High Tech Crime Sub Group is, at least in part, attempting to address this by starting the dialogue on key issues.

The CPS is also represented on a range of other multi-agency groups, such as Home Office Internet Task Force, which was set up specifically to deal with child protection issues on the Internet.

Involvement in these groups has provided an invaluable resource for the CPS in taking forward its own High Tech Crime Training strategy. The aim of this strategy is to raise the profile of high tech crime within the CPS and train a group of specialist high tech prosecutors across the country. These prosecutors will then be able to provide advice and guidance locally on cases involving high tech crime.

However, if the trends continue and there does not appear to be any reason to doubt this, then in the long term all prosecutors will need a fuller understanding of high tech crime issues. Furthermore, as technology develops so the training and guidance on such issues will need to develop. Therefore, it is crucial that the partnerships that are being formed with specialists and experts in industry both nationally and internationally are maintained. For it these individuals who have the best chance of predicting what lies ahead on the technology horizon.

I think it will become apparent that cyberspace is simply not just another form of communication whose legal problems can be accommodated within traditional structures. There is a new world out there and we do need to re-think certain approaches and be imaginative in our response. We are tackling these and the SFO is playing a valuable part in all this.

**Turning specifically to cyber-fraud:** Firstly I should make it clear that electronic crime – or cyberfraud – isn't really a separate new category of offence. It is merely a new way of committing very old and familiar offences. The World Wide Web is a wonderful thing; it is a new and dynamic tool that we use daily to get information, to communicate with people across the globe, to transact business and of course anyone who has a modem and a computer can access it. There is no filtering process to keep out those who are not fit and proper from offering their services, hacking into other people's systems and generally causing world-wide mayhem and enriching themselves in the process. The

tools that international law enforcement have at their disposal are geared to the more sedate and conventional means of communication and offering investment opportunities. There are sophisticated regulatory rules and procedures in place to stop the criminal, the incompetent and the insolvent from offering investment advice and taking your money. Those work when those people are in one definable jurisdiction and transact business in another, definable jurisdiction.

Out on the Web, the practicalities of stopping people who could be based anywhere, whether in a regulated jurisdiction or not, and whether they are who they say they are or merely a front for “Fraudsters International Inc” are obvious.

The main danger for law enforcement from the Net at the moment is the proliferation of paedophile pornography that has burst onto it. I mentioned the wOnderland case: the Gary Glitter trial two years ago highlighted what to most of us was unknown territory. According to police sources, international paedophile rings have been using the facilities offered by the web for anonymous, world-wide communications to network with each other, to send the most appalling images round the world and build up their network of contacts with each other, and, much worse, with the poor child victims of this disgusting trade.

The opportunities that the web offers for fraud are no less obvious, if less horrifying. Hacking and stealing data are two, specifically computer-related forms of crime. Laws in different jurisdictions differ as to whether this is theft or not; many countries have no laws to prevent or punish criminals hacking. In the USA, the Justice Department found that a hacker had transformed Janet Reno, the former Attorney General into Claudia Schiffer on their Web-page ( I doubt whether Ms Reno would have complained about that); the New York Times found its web copy had been altered and the CIA’s emblem was changed to read “Central Ignorance Agency”. In other cases, contractors who had fallen out with their principals, electronically repossessed the firm’s software. The intriguing element about stealing computer data – or electronic piracy as it is sometimes known – is that it enables data to be stolen without depriving the owner of it and without him knowing it has been stolen. The lack of security in systems, even those in the highest places, is notorious and seemingly impossible to render impregnable. Some months ago, the Halifax Building Society share dealing service reported that, by inadvertence rather than fraud, its security systems had broken down and it had to be suspended. Egg and Barclays Bank had similar experiences.

Indeed, some laws actively impede the activities of law enforcers while trying to preserve “rights” of the individual. For example, the EU Privacy Directive has the unwanted effect of putting curbs on police surveillance and monitoring techniques. The UK Regulation of Investigatory Powers Act, 2000, illustrates the fine dividing line between the competing aims of encouraging people to encrypt their electronic communications for better security and ensuring that law enforcers have the right to secure passwords and encryption keys to break the confidentiality of the encoded messages used to facilitate crime.

Criminals have from the first targeted computer systems and exploited their lack of security. At a recent conference a Canadian computer crime expert, David Toddington reported that criminal organisations are actively engaged in recruiting the best hackers available. They have at their disposal the most advanced cryptographic tools allowing them to communicate with relative security themselves. In addition, they have “wiping” software, to enable them to destroy incriminating data. There is an abundance of information freely available on the Internet on how to commit computer crime and defeat investigative efforts.

What can be done when an organisation has been attacked? Ed Stroz of the FBI offers the following -

- ◆ If there is indication that a computer crime has occurred, report it to the authorities immediately.
- ◆ The data itself, access logs, keyboards etc are part of the “crime scene” and should be secured. Don’t contaminate the “evidence” by wiping incriminating fingerprints etc.
- ◆ Do a risk analysis of the company to establish the boundaries of any damage.
- ◆ Prepare a cost account to assess the impact of the crime.
- ◆ Law enforcers – crime prevention officers in the UK– will be able to help with a “threat assessment” and advise on better security to prevent a future attack.

When the Internet becomes the tool of the investment scam, the scale of the problem assumes mammoth proportions. The speed at which the opportunity presented by Internet commerce is being taken up by both consumers and business is breathtaking. Commonly cited figures show that by next year, revenues which financial services companies earn on the Internet will total something in the region of US\$ 23 billion. Those companies which use the Internet for business-to-business purposes will earn revenues of something of the region of US\$ 66 billion. Those which sell their wares to consumers will realise US\$ 7 billion

The prospective market that can be reached on the world-wide web is in the region of billions of people, the majority of whom are completely unsophisticated when it comes to financial services products. New techniques for detecting, preventing and punishing this sort of investment scam must be found. The relative anonymity of the Internet increases the opportunity for cyberfraud. Anyone who wishes to inhibit fraudulent activities on the net must be able to come up with a system which can not only verify the identity of customers but that of the website itself.

Arthur Levitt, the former Chairman of the Securities and Exchange Commission in the States, has said that he was concerned by “the great influx of new and relatively inexperienced investors” who are drawn in by the ease and speed of Internet share trading. They are also being attracted by emotive advertising. Online share trading increases in volume by the second and now makes up a quarter of all private investor transactions in the US (more than 7 million Americans trade this way). Complaints to the SEC more than trebled last year and there have been more than 100 cases so far involving fraudulent Internet practices. Most of these traders are amateurs working from their home PCs or their employers’ terminals.

### **What can the law do about it?**

In the UK, the 1968 Theft Act provides a maximum penalties of seven years imprisonment for dishonestly appropriating property belonging to another with the intention of permanently depriving that person of it and ten years for dishonestly obtaining property by deception. The 1978 Theft Act covers dishonestly obtaining services from another by deception. Common law can be used for conspiracy to defraud where two or more people commit the crime and this carries a prison sentence of up to ten years.

Old style financial scams – advanced fee frauds, pyramid schemes, “pump-and-dump”, share pushing and get rich quick schemes – have been given a new lease of life on the Internet. The most colourful cases to date have come from the United States. In 1996, a fraudster agreed in court to repay US\$ 12 million that he had collected in a stock manipulation scam. And in April this year, a company’s share price jumped 30% following the release of false takeover information on the Internet. In another US case last year, a newsletter author allegedly made profits of US\$ 172,000 from sales of shares in one company and US\$ 573,500 from another; both companies failed to perform as hyped and the new shareholders lost much of their investment.

There is the now notorious case of a 14-year old schoolboy in New Jersey, Jonathan Lebed, who made an illicit profit of \$272,826 by buying shares in 9 thinly traded companies, posting misleading messages on Yahoo! Message boards touting them and selling typically within 24 hours after the postings ramped the prices. In some cases, he would post a sell limit order to ensure that he would not miss the stock’s increase when he was in school the next day. Prosecuted by the SEC, he settled on a no admit/no deny basis with the regulator by agreeing to forfeit his profit and pay interest of \$12,174.

Deceptive investment opportunities don’t even have to concern real companies. One “cybervigilante” claims to have uncovered a biotechnology company which in fact sold cat litter and “the largest corporation in Nevada” which was nothing more than a two-man air conditioning repair shop. In the US (again) there have been reported cases of bogus investment banks appearing on the Internet which offer high interest rates and disappear as soon as funds have been attracted. Copycat sites look genuine: in one case, the share pusher had posted the information on an Internet site which was dressed up to look like a news report from a reputable financial information provider.

The Internet has certain inherent features which make it ideal for fraudulent purposes: cost effectiveness, breadth of reach, difficulties authenticating identification, anonymity, ease of personalising appeals. A fraudulent investment scheme may be advertised relatively cheaply on a credible looking website or by mass e-mailing and reach millions of people across the world making it much easier to locate those gullible enough to part with their cash.

In 1997, a phoney US investments scam making false claims about a high tech start up company attracted nearly 100,000 people to its website, 3000 of whom e-mailed for

further details with 150 sending in money. In three months the con-man netted US\$ 190,000.

The inability readily to determine the authenticity or location of a claimed identity prevents even the most cursory assessment of the validity of a communication. This works both ways; neither the seller nor the buyer can be truly certain of the authenticity of the other. In such circumstances, opportunities for fraudulent activity emerge. The fraudster composes a reputable entity to give himself credibility. Thus, sites which are assumed to be owned by a legitimate company can be established to take orders and credit card details and either process the transactions to receive payment or use the credit card details fraudulently. To inspire false confidence, fraudulent sites have even been known to warn viewers of scams. A hacker-fraudster “hijacking” the web page of a reputable investment advisor and using it to advertise a fraudulent scheme might well fool even the most wary.

The one area where the user at the moment needs as much reassurance as possible is that the Internet is a secure place to do business. I have already mentioned the difficulties the banks and building societies have experienced. Citibank is still recovering from the case of Vladimir Levin, who hacked into their system from his computer in St Petersburg, disguised himself as a bank and organised wire transfers of US\$ 12 million to accounts under his control. There are of course devices such as encryption and steganography designed to improve the security of the system. But any system which can be used to protect legitimate messages from prying eyes can equally be used to hide criminal transactions from enforcement eyes and, as I have mentioned, the extent of the legality of encryption and steganography is still the subject of ongoing debate. In the UK, Citibank’s new Internet banking service, Direct Access, is protected by high level encryption but its terms and conditions often warn customers that “the use of such levels of encryption may be illegal in jurisdictions outside the UK”.

### **What other scams can the Internet fraudster get up to?**

Well, why not set up your own Internet bank or another financial institution of your own. Nowadays anyone with the money can buy for example an international business company (IBC) over the Internet. These are corporations with no jurisdiction, no accountability and often with no traceable ownership and as such are the ideal vehicle for fraud and money laundering. Choosing the jurisdiction carefully, the IBC owner can then set up a bank account again via the Internet for that corporation, and thus has a fully functioning financial concern which is almost impossible to monitor.

Using his bank’s Internet facilities, the criminal can then access his accounts and its funds from anywhere in the world and spend it in anyway he likes – leaving no audit trail for law enforcement to follow.

Criminals can take advantage of the free nature of the Internet to set up their own banks, domiciled in any location which promotes itself as regulation free, allows anonymous accounts and will not question large deposits.

### **Is there no way to police the Internet?**

People sometimes assume the Internet is not governed by any law or regulation but this is not the case: in fact the Internet is governed by too many laws and regulations.

For instance, the UK authorities have so far taken the view that any website that can be pulled up onto a screen in the UK has to comply with the relevant UK legislation. The UK legislation includes the Theft Acts which I referred to before and of course the Financial Services Act which authorises those who sell investment products those to the public. Multiply this by the countries in the world and the task facing the compliance department of any financial institution is daunting. They have to make sure the products and services on offer comply with the regulations in force in every jurisdiction in which that website can be accessed. There is huge room for confusion. In the US for example some of the existing online “banks” are not covered by anti-money laundering legislation, as they purport to be merchants selling a service rather than a financial institution.

The Internet of course is a wonderful place to sell impossible dreams to unsophisticated investors. Some of you today may not have heard of Prince Lazarus Long, also known as Howard Turney, the man who promoted “The Principality of New Utopia”. It is hard to believe that people with sense let alone money were prepared to invest anything up to US\$ 20,000 to become a citizen of this totally non-existent tax free island paradise in cyberspace which was offering the promise of their money being paid back with 9.5% interest and the chance to invest in a 350 million dollar bond offering. Two Britons were among a group of about 20 investors from South Africa, Lebanon, Italy, Australia and America who were prepared to hurl their savings into cyberspace. The SEC labelled the Internet investment scheme a “fraudulent endeavour” and shut it down, freezing all the money collected.

Another non-existent cyberstate is the Dominion of Melchizedek, several of whose leading “statesmen” were arrested at the end of 1998 in the Philippines. The Dominion of Melchizedek was part of a Californian based confidence trick run by US convicted fraudster John Gillespie, an Australian claiming to be the Navy Minister of Melchizedek, a man called Chu Chin Chee, a Malaysian who passes himself off as a Hong Kong diplomat, and Stewart Mason-Parker a British lawyer and former Hong Kong prosecutor who left the colony allegedly with considerable debts. The group had talked hundreds of Philipinos, Chinese and Bangladeshi’s into parting with over £2000 each for travel documents that they were told were internationally recognised passports. Others had paid large amounts to obtain government jobs on the non-existent Pacific island that the Dominion claimed was within its jurisdiction. Supported by bogus information on the website which claimed diplomatic recognition from first and third world countries the gang had taken more than £1 million before they were picked up. Melchizedek first emerged in 1990 and since then has been responsible for a series of scams. In 1995 the Bank of England raided its London offices which were offering get-rich-quick schemes backed by a Melchizedek-registered bank. Investors were told the bank’s assets were underpinned by US treasury bonds. They turned out to be “financial instruments” issued by the extinct Weimar Republic. Its latest incarnation on the Internet is only the latest of many different incarnations for this most elusive of territories. As well as international

travel documents, the “cyberstate” offers to incorporate banks, insurance companies, trusts and private corporations for a few thousand dollars. It also advertises university degrees and lawyers certificates.

### **What can be done to prevent such scams?**

The old rules are usually the best. Deals that look too good to be true usually are. You should remember that generally the higher the promised return, the greater the risk. The Internet itself is unregulated; the Financial Services Authority has compared it to a galactic car boot sale. Anyone from anywhere can set up shop and offer you anything for sale over the Internet. But if you buy shares or any other investment from an Internet firm that is regulated in the UK then the firm is subject to UK laws and you have a measure of protection including recourse to compensation should things go wrong. If you buy shares from a firm based outside the UK you need to bear in mind the difficulty and expense of pursuing a complaint. The Financial Services Authority advises that you find out first where the firm is based, whether it is regulated and which country’s laws apply in the event of a dispute. The FSA has warned investors that unscrupulous operators can easily copy a site run by a legitimate firm and set up a bogus one of their own, so take a close look at a website that you’re thinking of doing business with. The address may be similar to one used by a well known company, but might have an unusual overseas location or contain additional misleading letters. Watch out for the pump and dump stock scam where shares in small companies are touted by people who fail to disclose the fact that they are paid by the companies themselves. Once investors have poured cash into the shares which pushes up the price the insiders sell the stock for a healthy profit. When they start to sell the share price tumbles and investors are left high and dry

A message appeared on a Yahoo! stock board in April, alerting investors to the forthcoming takeover of a Californian based Internet company for nearly twice its market value. The message even had a link to the Bloomberg financial site, thus giving the impression that it was a legitimate story but it was not. It took two hours for the hoax to be exposed but within that time dozens of investors were swindled.

### **What experience have we had in the UK of such scams?**

As far as the SFO is concerned, almost none at all. What America sees today, however, Europe experiences tomorrow and the UK will, I am sure, shortly be seeing a number of UK-based cyber-frauds. In essence, as I have said, the crime itself is no different from any other terrestrial fraud; use of the Internet affects the means and the size of the target, in the case of investment frauds.

The problem of enforcement through the criminal courts will be largely one of jurisdiction. Identifying the source of the fraud and being able to arrest, interview and eventually charge the person responsible, depends, as in so many other internationally-based frauds, on the location of the fraudster; whether the jurisdiction in which he is located is one which is co-operative in matters of judicial or legal assistance to overseas authorities and what arrangements are in place for extradition.

Criminals know perfectly well which the jurisdictions are where investigators who finally catch up with them will be stopped in their tracks by such devices as notifying the account-holder (usually the criminal himself or his stooge, or “nominee”) of the request for assistance and the opportunity to contest it

This is one reason and one area which highlights the importance of good, effective and speedy channels of communication between legal and investigatory authorities; and, on a more formal basis, of mutual legal and judicial assistance to secure the production of evidence in a form which can be admitted in a criminal prosecution. It is a matter of great concern and dismay that there are still jurisdictions, even within Europe, where assistance is not as readily forthcoming as would be ideal. Where letters seeking information go unanswered, or where judicial process can delay the transmission of information – in some cases, until after a trial is over. ( In Liechtenstein there are no fewer than 17 avenues of appeal which the account holder can use to delay access to his bank account or details of his secret trust or “anstalt”.) Out of the 15 member states of the EU, there are 11 which will not extradite their own nationals abroad. There are disparities between jurisdictions as far as extraditable offences are concerned. Many continental jurisdictions do not recognise private sector corruption as a crime and will not grant a request for extradition where that offence is alleged. There are differences between jurisdictions with regard to whether assistance can be afforded, depending on the stage at which proceedings have reached.

### **Working with the police and the Serious Fraud Office**

From time to time, as compliance officers, it will fall to you to report crime to the authorities. We don't actually know how much “fraud” is being committed in this country. Part of the reason for this is that not all fraud, even substantial fraud, is reported to the authorities. I am conscious that there is a disincentive to report fraud when police forces are under-resourced and harassed officers are bound to explore with a complainant whether there are civil avenues of redress that can be pursued, or to redirect a complaint from one police office to another, sometimes over several counties, until the complainant feels it is not worth the candle and gives up the unequal struggle.

But principally fraud does not get reported because it is not felt to be in the interests of a financial institution to report that it has been the dupe of a clever criminal or con-man. Weaknesses in internal systems, in management and supervision will give an unwelcome impression to its customers and potential customers that it is not safe to do their banking business over the phone; or over the Internet. Cut your losses and get rid of the internal fraudster is a tempting thought. If the fraud is from an external source, is reporting it to the police likely to get you your money back?

Most public-spirited people will report fraud. There is every possible reason for them to do so. The more knowledge that can be disseminated about prevalent frauds, of potential hazards to the system as a whole, the more the financial community will protect itself for the future. Fraudsters who stay unidentified and unprosecuted live to defraud another day – and another victim.

Where a firm is the target of fraud, we, like the police, are immensely assisted by those in compliance areas in firms who are able to describe the way of working in the firm; the key responsibilities and functions of personnel and departments. Preserving documentation and tapes of conversations will be of great benefit to the investigation. Don't write on original documents – you would be surprised how often a vital record of a conversation between the Head of Compliance and a suspected employee has comments in the margin written at the time of or after the interview. You may remember the “Yes Minister” episode, where Jim Hacker writes, euphemistically and, as he fondly hopes, amusingly, “round objects!” in the margin of a document. “Who is Round, and to what does he object?” asks Sir Humphrey disingenuously. A judge may not take such a benign attitude if your document is similarly adorned and read out in court.

One initiative you may be aware of is the Accredited Investigators initiative, whereby institutions pay private investigators or accountants to carry out the initial stages of the investigation, drawing together the documents, interviewing witnesses, perhaps preparing their witness statements and then providing a package to the authorities. In practice this has been happening for some time particularly where banks or other financial institutions have been the victims of fraud and it has, to some extent, shifted the burden from the public to the private sector. In theory this should release fraud squad officers for more active work, and allow them to deal with more cases at any one time. There are some immediately obvious drawbacks to the scheme, not the least being the implications for disclosure of material seized by non-police investigators prior to the involvement of the criminal authorities and the criticism that the only frauds that are investigated are those where the victim is able to pay for the investigation. I hope these difficulties will be overcome.

**To conclude.....**

“It is a very familiar truth that regulation is national and business is international and business is more international across cyberspace. And frankly that gap is opening all the time” said Sir Steve Robson, Director of Financial Regulation and Industry at the Treasury. Fraud involving the Internet has been seen as less likely to affect sophisticated institutional or wholesale investors; the more likely targets are less knowledgeable retail investors.