BILETA

14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

Use and Abuse of the Internet in Fraud and Money Laundering

Nigel Morris-Cotterill
Solicitor, Compliance Consultant
Author "How not to be a money launderer"

Nigel Morris-Cotterill

Nigel is a solicitor and was formerly an associate with a small City firm. His clients included a range of financial services companies. He is now a consultant with a small firm and an in house lawyer in financial services and technology companies. Nigel acted for the first person, a professional advisor, to be charged in the UK with money laundering as a stand alone offence.

Nigel writes and broadcasts for major media outlets such as BBC1, BBC World Service, R4, R5Live, Classic FM, Sky News, IRN, Austria National Broadcasting Service and, in print, The Times, The European, The Independent, Sunday Business and many other print and broadcast units including professional and academic journals. He has been interviewed by many leading newspapers and magazines - for example, the Observer and The Wall Street Journal and others, less internationally known, from places as diverse as Gibraltar and Bermuda. For several years he was a contributor to Money Laundering Bulletin.

In addition, Nigel designs and delivers money laundering compliance and risk management training courses and seminars for the banking and wider financial services industry. His courses are hosted by most of the biggest names in financial sector training.

Nigel has formed his own risk management, training and compliance consultancy, Silkscreen Limited. He is author of "How not to be a money launderer", described by Legal Abacus (The journal of the institute of Legal Cashiers and Administrators) as "a book everyone in business should read.". The second edition was published in 1999.

The Ball Point Pen. It's a simple device: Sticky ink is forced into a small tube and a device is…

Am I in the wrong place? There are puzzled looks. Is this the wrong technology for this conference?

Should I be talking about computer technology, then? OK. What happens inside your computer is really fascinating. Of course, it needs electricity but once you have plugged the computer into the wall and pressed the on switch, the power comes along the cable into what is called a power supply. That does two things: it converts the current from a high voltage to a low one, often from 220v to 3.5v. And it converts it from Alternating Current or AC to Direct Current or DC. Alternating Current is really interesting because….

Actually, no matter how interesting it is to people who need to know, it is of no relevance here. And for most people, there is no need to know how the internet works, either.

But when it comes to considering the policing and regulation of the Internet, there are some important consideration which arise out of how the Internet works.

I am not, however, going to deliver a technical paper. In part this is because I am far from qualified to do so. I will, however, highlight some of the technical issues as we examine the legal issues which form the basis of this paper.

First, a two very short questions: do we need to regulate the Internet and, if so, why?

In the USA, the question of regulation has reached a crossroads. Only a few months ago, the main issue on the internet appeared to be driven by fiscal concerns: where will goods and services delivered by Internet be taxed? This is a topic I will return to later.

However, more recently, the American concern turned to a much more American concern: that of free speech.

And then, only a matter of a few days ago, the Americans finally woke up and did something about fraud on the Internet. We will be looking at these issues in brief today but, in the published paper, there are rather more detailed comments.

There is a great divergence of feeling, internationally, about the desirability of taking regulatory steps in relation to the Internet. Let me outline some of the opposing arguments:

I am a lawyer dealing predominantly with questions of compliance with money laundering laws. I tell financial services organisations that there is no place for allowing discretion - if a system is to work effectively, it must, I argue, apply equally to all, regardless of the circumstances. The reason it must work effectively is that it is for the good of the organisation - the penalties and other effects of non-compliance can be devastating for a company. In this way, the company may be taken as a microcosm of society.

However, I am also a driver. I am a good driver. I am also a very fast driver. I take part in motor sport. I drive with great anticipation and caution. And I can see no reason why, where conditions are appropriate, and I am in the right frame of mind to do it properly, the speed at which I drive should be regulated with reference to an arbitrary speed limit. I do, however, see that drivers who are less able, or who do not recognise their own limitations, or those of their vehicles or others or other adverse conditions, should be penalised for inappropriate driving. The problem, here, as is obvious, is that I am advocating a discretionary system.

The reality is that ordinary people rail against regulation of themselves whilst advocating regulation of others. Freedom to do as you will is acceptable so long as

a. it does not impact upon me; and

b. it does not prevent me doing whatever I want to do, wherever and whenever I want to do it.

Clearly, this is not the mark of a civilised society. Regulation of some sort or another is an inevitable consequence of congregation for the simple reason that there are only two sides of this coin: regulation or anarchy.

It has often been said that the Internet is anarchic. This is not actually so. But few understand how much regulation there actually is. And how to make it work.

The most obvious problem with the Internet is that in Cyberspace, everyone knows your name but no-one knows who you are. Anonymity is not merely easy but almost automatic. The Internet actually promoted the use of false identity.

In this way, it is no different to the "Citizen's Band" radio craze of the early 1980s. Everyone had a "handle" - a self chosen nickname: a false name.

Before setting out to blame the Internet for a rise in all manner of evil, it is first important to decide whether it in fact creates any evil.

I would argue that it does not create any new evil but merely offers a new manner of presenting already unacceptable conduct.

The fact is that people are always taken in by a kind of magic. To see the printed word must have greatly impressed those who had only ever seen books bound from original manuscripts. The advent of mass market printing, in books and later newspapers and journals undoubtedly gave credence to all manner of material, true or otherwise. There is the often repeated statement "it must be true, it was in the paper." In recent years, this is often said with sarcasm but it is not long ago that most people did not read a daily newspaper and when they did it was because of some momentous occasion such as the Coronation or war.

Broadcast media has, and in the UK at least, remains a means of securing truth. And as a result, there has within the past few months been several cases of extraordinary concern over the falsification of information in both documentary programmes and those involving audience participation. This reflects the reality that many viewers believe what they see on television unless it is markedly entertainment.

I can tell you from personal experience that a little high profile radio coverage goes a long way and creates a degree of credibility that can exceed reality.

I know nothing about buildings subsidence but I used to work in a firm where a solicitor specialising in these cases also worked. He was due to fly to the USA when, the day before his flight, a BBC Consumer programme asked if he could do an interview shortly after the time his flight was due to leave. I stepped in and overnight read several briefing papers and articles. I handled the interview without fluffing and what I said was correct - and I said that my colleague was the expert in the area. If I had been asked the same questions a day or two later, I could not have answered. However, some two years later, people were still ringing me asking for advice.

The fact is that the majority of people will believe what they want to believe from broadcast media - a point not lost on marketing men who put a late night, occasional advert on television and then mark their packaging "As Advertised on TV" or even "As seen on TV."

The perceived endorsement of having been "on TV" is a powerful stimulant for the consumer.

Elderly people, in particular, do not realise the extent to which they are targeted by advertising. A personalised junk mail letter is sometimes received with pleasure: I have heard "the bank wrote to me to ask me if I would…." These are people who grew up with the bank manager in the cupboard and believe that the bank offers advice when, now, it generally merely makes sales.

What we are seeing here is a culture gap: people who do not understand the power of modern marketing. They do not realise that hundreds of thousands of letters can be individually addressed and mailed in a single day. They believe that persons who have professional standing are honest and when they make a recommendation, they are making it for the customer's best interest and, if a profit is made on the way, so much the better.

Finally, there is the middle aged generation: people like most of us reading this paper. We grew up with a computer being a thing of wonder. I remember being taken to Teesside Polytechnic on a Sixth Form College outing to see a computer. It was huge. It took up a massive room and required arcane commands to make it do the simplest things. We learned to trust what the computer handed out. In a modern version of "It must be true it's in the papers..", the computer industry persuaded us that if it is on a screen, it is true.

So, as the Internet becomes a mixed medium of broadcasts, news content and mass mailings, all delivered on a screen, we find that each of these means of suspending the natural cynicism of the reader have combined to make the Internet user a willing victim of internet fraud.

Internet fraud is easy. In my book "How not to be a money launderer", I show many ways in which criminals make the money that they launder. In one example, I show details of an e-mail scheme that recommends a particular stock. I investigated that e-mail.

Let me tell you how simple it is for a criminal to make a scam work:

There are several internet service providers around the world who will let you set up an e-mail account without any identification at all - or will allow set up with the creation of fictitious details. Are they hard to find? Now: they advertise on all manner of websites, often banner swap schemes. These are legitimate businesses. They do not condone the use of their e-mail or web systems for fraudulent business and, in many cases, will have specific exclusions for spamming or other antisocial or even illegal activities. But there is a time lag between a scam being put into operation and the ISP taking steps under the agreement.

OK, so the fraudster can set up his WebSite for free. Next, he books an internet domain name. The cost of doing this is US$70 per domain. Many free ISPs will also host domain names for free. Others will require a fee of perhaps US$20 per month. Many are less. He will only need it for a month.

Next he sets up a Public Relations agency. This will mail out lots of e-mails promoting a stock. The PR agency will have its own domain name. So far, the fraudster has spent under US$200. He will now buy a mailing list. This might cost US$1500 for a large list. He does not need it to be a highly qualified list. In fact, he wants internet aware but otherwise unsophisticated persons to receive it. Because what he does next is a paper thin scam.

The Over the Counter market in most countries is at the margins of the regulated area. Often little known companies, the stock is highly speculative. But these are companies that

appear and disappear with alarming speed. Some survive and go for a full stock market listing but many are troubled companies trying a last ditch attempt at solvency or even new companies with no track record looking for start up capital for a barely formed idea.

But OTC stocks are traded, in large number, by unsophisticated persons who know little about the business and nothing about the company save what is contained in a e-mail.

So, a WebSite is created that presents a picture of the company. The OTC pricing is shown by a cross reference to a genuine reference agency such as Reuters (who were used in one case I am examining).

The Website can have all manner of legitimate images placed in it. The code to import an image from a legitimate WebSite to a copycat WebSite is less than one line of simple wording.

For example, to import a graphic from my WebSite, the designer of another WebSite would merely have to insert in his page design the line:

<IMG SRC="http://www.countermoneylaundering.com/blair.gif">

This will import into his page a picture of…..oh, go and look at it for your own amusement!

Such techniques improve the apparent legitimacy of the page. It is simple to import the logos of legitimate organisations. This technique, called "in-line images", is one of the strengths of the Internet protocols but it is open to wide abuse.

Next, the fraudster buys or acquires or even takes options over a large number of shares in the company and he uses an e-mail account that he sets up for single use. Sometimes he invents an address: it is commonplace for junk mail messages to be issued with forged return addresses. This is designed to secure a delay in tracing the fraudster but also the choice of address is a way of giving credibility to the scheme. For example, Yahoo provide a stock market quote service for US Stocks. Many fraudsters set up either a free Yahoo mail account or even falsify a Yahoo account name.

He sends a strongly worded recommendation to buy the stock. He will often include messages that stock can go down as well as up and even make reference to a US Code that says, he will claim, that so long as instructions as to how to be removed from a mailing list are included a message cannot be considered to be spam.

In some cases, the note will say that it is issued by a paid for PR agency that has taken its remuneration in stock - usually 50,000 or even 500,000. This may be true. After all, if the scam works, the stock will be worth considerable more in a few days than now - or in a few days after that.

So, the scene is set.

Out of the millions that receive the e-mail, several hundred will buy stock over a period of a few days. The purchases will lift the stock price. Volumes will multiply over and over, The cautious who watch the stock before committing will see it move a little and put their weight behind it. This works best where large percentage gains can be made - so extremely low value shares are a favourite.

And then the fraudster will dump the stock he bought before he began the scheme, perhaps

even before settlement day on his trade. He may even be taking the role of market maker, in effect setting the price and selling off the stock he bought.

The incomers will see the price collapse. The company, more often than not, will not last much longer. The WebSite will be closed down because regulators or the ISP will have been warned. The e-mail addresses will be shut down because the allocation agency has not been paid or because Regulators issued a Cease and Desist notice. All the addresses e-mails purported to come from will prove to be false trails.

But there are trails. I have followed one back to an individual in the USA.

And so have the Prosecuting authorities in the USA. In February 1999, the Securities and Exchange Commission brought proceedings against several of those involved in the marketing of Interactive MultiMedia Publishers Inc. The company was pumped to the extent that it eventually was valued on Wall Street at US$40m. In the USA, companies make "filings" with the SEC, these are little more than press releases but are supposed to be non-misleading. The SEC said that the company's filings were fraudulent, inflated the value of its assets and said "marvellously exciting things were happening when they weren't." The SEC has charged the President and Chief Executive Officer with insider trading, financial fraud and stock manipulation and issuing false press releases to raise the price of the stock. Three others have been charged with securities fraud - it is alleged he proclaimed the merits of the stock on the Internet but failed to declare that he was being compensated for his enthusiasm. Further, another person, a stockbroker, is charged with aiding in the setting up of the scheme. It is not known how the men will plead.

The reality is that there is nothing new in any of this: it is simply a new and currently more convincing way of conducting the old fashioned "boiler room" stock "pump and dump" fraud.

So, is this still happening? Of course it is. At Appendix A, I have put two e-mails which are clearly circulated without any form of discrimination. This suggests mail-outs of millions. I have added footnotes with comments. There is no reason to suspect that one or even dozens of prosecutions will result in fraudsters abandoning their practices. One of the advantages of the Internet is personal and geographical anonymity. It is not necessary to know where you are for a person to communicate with you. That freedom is open to abuse as a person can set up a fraud and collect the money in a false name in a distant place. All he has to do is gain access to the money. This is not difficult.

The simplest internet scams are those that say "send money to this address". I have not added examples to this paper because they are legion. Anyone with an e-mail account will, almost certainly, have received at least one document claiming not to be a chain letter. Or offering you a once in a lifetime opportunity if you wrap five dollars in paper and send it to an address buried deep in the e-mail message. The return addresses will not work, or will be free mail service mail boxes which fill up within minutes of the mail-out.

I have put several examples of these e-mails in an appendix in "How *not* to be a money launderer".

So, we have established that the Internet is a vehicle for fraud. What of other evils?

The Internet is a medium for the rapid dissemination of information. Everything on the Internet is in binary code stored on and passed between machines. The machines have no concept of right and wrong and have no means of knowing whether the pictures stored on it are innocent family photographs or pictures of depravity. The machine does not even know that the information stored on it is a picture. The machine does not know whether the

information which passes through it is a coded or open message. It does not know whether coded messages are permitted in the format used. In short, the machines have no conscience.

However, sniffer programs can identify certain types of information as they pass by. These are the programs that the raise concern about security on the Internet. It is claimed that criminals use sniffers to monitor internet traffic, to look for strings of numbers that are credit card details. One of the truths in fraud prevention is that there are a lot of bad guys and not a lot of good guys and, as a result, the bad guys get the best technology first. Governments are concerned about encryption and all manner of excuses are made but the simple truth is that the reason they do not want complex encryption is because their own sniffer programs are not good enough to break the codes fast enough.

Encryption is one of the battlegrounds when regulation of the Internet is considered. This is because of the USA stance that 128-bit encryption cannot be exported. Actually, this is a myth. The code cannot legally be exported in electronic format. So Microsoft's 128 bit encryption for Explorer will not allow download to a domain registered outside the USA.

However, PGP128 has been exported on paper and re-keyed in Europe and is now available for use.

France legislates against the use of encryption in its entirety but there are exceptions made.

The UK is talking about banning encryption, basing its arguments on the supposition that encryption provides a shield for organised crime. In fact, this is an excuse. Whatever the real motives for the UK's stance, to blame organised crime is merely to play on the fears of the majority to gain support for a willing reduction in personal freedom.

There is nothing illegal in an individual sending a message through the post in code. Indeed, given the propensity of politicians to say one thing and mean another, it is arguable that they use code all the time. I am embarrassed to admit that I cannot recall who gave following example to the Symposium on Economic Crime in Cambridge, England, in 1997: a criminal gang wanted to send a message giving details of the arrival of a shipment. They sent an open e-mail message "Dear X, I am glad you will meet my daughter Y at the airport on Sunday at 5pm. She will be travelling on flight number ZZZ. Attached is a picture of her." Sure enough, attached to the message was a scanned photo of a girl. Agents could not believe their luck. The bad guys had made a rare mistake: an open appointment with the drugs, the courier and the bag-man (or girl) complete with photo of one of them.

Of course, no one except the police went to the appointment. The information was not in the message. It was in the photo. A digitised image is made up of many thousand of individual dots, perhaps 4800 per inch. Each dot is made up of information: the colour is a string of numbers. The criminals had changed the colour of one dot. Amongst the range of colours on the photograph, the change of one dot was invisible to the eye. But not when the source code was analysed. In a range of brown, one blonde dot will not show up, but in a list of numbers, where there are many the same, it will stand out. The colour code for the changed dot gave the location and time of the real drop.

This is not encryption. There is no hope of enforcement agencies spotting the correct information, and then working out cross references based on an old fashioned code, before the drop is made. No form of regulation will prevent this happening again.

And this is only one example of clever use of simple technologies.

The Internet can be used for blackmail. Look at the picture at http://www.countermoneylaundering.com/blair.gif (referred to above). This is a photo that I doctored in a few minutes using software that costs less than UK£50, on my normal desktop PC. This is not a complex process. It would be a simple matter for me to take a photograph of a person and paint him into a compromising situation. Amazingly, because the computer works by changing the colour of an individual dot, there is no shadow, unlike traditional montage. Such a photo sent over the internet does not suffer from the more usual signs of fakery. Again, no form of regulation can protect against this abuse.

It is clear that regulation will not prevent the abuse of the internet because the Internet is a truly borderless medium but laws are national. So, in the same way that there is no genuinely international law, there can be no genuinely international regulation of the internet. The World Trade Organisation could take a stance, as could the UN and unions such as the EU. But these take time and are always embroiled in national interest debates and in the meantime, the criminals make hay.

So, is there anything that can be done? In the infamous *CompuServe* case in Germany an ISP was held liable for information posted by third parties. This must, I think, be regarded as a rogue decision. The Internet cannot function if ISPs are to be held liable for all content published or passed through on them. I can understand some of the rationale of that decision: if the publisher of a magazine is liable for content of the letters column, then why should a server-provider not be liable for that which is posted on its servers? However, this is to deny the reality of the medium. It is not, I think, a Luddite response but it is no doubt fed by a wish that those who develop a new medium think very carefully about its consequences. I see nothing wrong in that. It should be regarded, in my submission as a call to caution even though the decision is greatly out of step with international thinking.

I can see, however, room for a development of this. E-mail systems can be programmes to prevent the transmission of more than a certain number of messages from a single domain. Most internet fraudsters, at present, do not set up their own ISPs. Thus the ISPs whose servers are used could be required to block more than, say, 200 messages an hour and more than one thousand per day from domain. There could be a requirement to make a report to a central authority of any message sent to more than, say, 100 people at a time. This can be entirely automated and need not require intervention by any ISP personnel. The US legislation on anti-spamming is piecemeal and makes little inroads into the overall problem.

The proposed Jersey legislation deals with stock promoting but misses the opportunity to make it an offence to deliver unsolicited stock solicitations by e-mail. Such a course of action could make it an offence triable in Jersey for a person outside the Island to promote a stock to a person in the Jurisdiction.

It has been suggested in private discussions with enforcement agencies from several jurisdictions that the correct jurisdiction for prosecution of an internet fraudster is that of the Victim. This is, in principal, attractive but misses out the practicality of securing co-operation in foreign jurisdictions. Many countries simply cannot afford to conduct cross-border investigations.

If anyone controls the Internet, it is InterNIC, the company that issues domain names. InterNIC will, if it is satisfied that a domain name is being used for fraudulent purposes or for other illegal activity, suspend the domain.

However, in all of these examples, there remains the single most intractable problem - that which is illegal in one country may not be so in another. Technical offences such as stock

promoting, and the invitation to invest without disclosing an interest, are not universal offences.

Most of the widely operated frauds are conducted from the USA, although I have recently had e-mails apparently from South Africa and Japan. The USA could take the simple step of making it a Federal offence to send unsolicited e-mails to any person outside the USA. The offence would be complete when one of the solicitations hits my desk. To prove it, all I would have to do would be to send a copy to a Federal Prosecutor in the USA. The OECD could try to encourage a similar tactic, perhaps by Financial Action Task Force recommendation.

In the meantime, the reality is that the Internet is actually quite well regulated by the ISPs who recognise that their reputations, and bandwidth, are taken up by the fraudsters. Simply forwarding the suspicious message to the abuse desk at the ISP (abuse@isp.etc) will often result in the suspension of service or at least a warning that the "from" address is fictitious.

Turning now to that most pure of financial crime, Money Laundering, the question of using the Internet for this activity is often raised as an excuse for regulation. Put simply, the Internet does not create any opportunity for money laundering which does not already exist. Again, the internet is merely a facilitator. At its simplest, every internet transaction is based on a telephone call. Every jurisdiction which has legislation affecting telecommunications, therefore has, in principle, legislation controlling what people can - and cannot do - over the internet. There may be an need for adjustments of definitions of traffic but, if fax (that is data) transmissions are covered, it seems to me that only the most contrary of judges will decide that the internet is a different sort of transmission. The blurring of distinctions becomes inconsequential when taking into account internet telephony. Indeed, the blurring became farcical with the development of digital telephone systems - I don't have figures but I would guess that in the developed world (in telephone terms) approaching 100% of telephone calls (other than calls within an exchange) are digitised at some stage of the call.

However, the Internet does offer opportunities for the money launderer. Money Laundering is all about messages. It may be a message about how to hide, move or invest money. Or it may be a message which does in fact move money.

Electronic money (which is not an internet phenomenon) is a new opportunity for money launderers. Or, to be more precise, it is a development of an existing method. A simple means of transferring cash from one state to another is by the use of a system called Hawalla or Fei Chi'en. The first means "honour" and is developed from Farsi. The Second means "flying money" and is developed from Mandarin. Readers of James Clavell will know the system - he calls it by its more colloquial name: "the chop system".

Put simply, all of these systems involve the payment of money in one place for collection in another. In the financial world, we have all sorts of names for this: money transmitters, automatic teller machines.

In the Middle and Far East, these Hawalla and the Chop are a part of the cultural heritage. And, like all mobile cultures, the communities take their heritage with them. So children sent abroad to work to support their families will often use these systems as an alternative to an expensive, patchy and often corrupt banking system. Where I live, it is five miles south to the nearest bank where I can use an ATM card, twelve miles east, six miles west and twenty miles north. In China, it can be a day's walk to a bank which is not even properly connected to a clearing system, a day's walk back and, if the expected money has not arrived, a further trip will have to be made. The Chop dealer is a local businessman who offers a valuable service. And at a cost of perhaps 10% of the amount transferred. When

the amount may be only a few pounds, the flat rate fees of the Western Bank where a waiter pays sends his savings home makes the regular repatriation of money impossible. Simply, the charges may exceed the sums which he accumulates on a weekly basis.

Hawalla and the Chop were developed to address the need to send money over large distances with a degree of security. This is because the money does not move. The Hawalla dealer in London sends a message to his counterpart in Bombay, for example, saying "Please pay to Mr X the sum Y, less your commission." The commission is, typically, 5% at each end. At some time in the future, the Bombay dealer will have a customer that wants money available for collection in London and so the transaction is set off. Eventually, there will be a settlement. In the Chop system, there is a token, "the chop", which provides a degree of security that the person collecting the money is the person entitled to it. The traditional method is the breaking of a coin. Half is sent to the dealer and half to the payee. The payee presents his half and is handed the money. The whole coin, albeit in two pieces, is the evidence of the debt from the London dealer to, for example, the Peking dealer.

For those reading this who are in financial services, you will realise that, with only minor modification, we have just described routine banking and services such as China Wire, MoneyGram and Western Union. The primary difference is that Hawalla and Chop dealers are, almost universally, not registered as money transmitters and are entirely unregulated.

But, because it is the message that moves and not the money, the Internet provides an increased opportunity for such parallel banking to operate amongst other communities.

And, before anyone claims that this is a uniquely Asian or South East Asian concept, remember your own birthdays and Christmases. How often did one of your relations say to your parents "I don't want to send money in the post. Can you pop £10 into an envelope for B's Christmas box from me? I'll pay you back later." And how many of you have an informal deal with your brothers and sisters to give money to your own children from them, and for them to give money to their own children from you? That's Hawalla.

Because of this availability of free transfer of value without transfer of money, foreign exchange transactions are avoided and there is no record of money movements through the banking sector. Accordingly, reporting requirements such as that adopted by the USA in the Bank Secrecy Act have no means of stopping or even identifying money transactions. Indeed, on the strict wording of the BSA, prima facie, Hawalla transactions would appear to be non-reportable: because the cash does not move. However, money transmitters, licensed or not, are in fact expressly brought within the ambit of the legislation.

However, how does the Internet help if the criminal wants to move the actual money?

Again, it is a medium not a primary cause of the activity. Again, it all revolves around messages. Money is, increasingly, data. The dematerialisation of money is a problem facing governments and others and causing widespread paranoia. Simply, if the Government doesn't know where the money is, how can it tax it. In the UK, after spending 18 years in Opposition claiming that indirect taxes were a regressive system (that is they attack the poor in greater proportion than they attack the rich), the Labour Chancellor, Gordon Brown, has in the past few days delivered a Budget which significantly moves taxation away from Direct (that is on income) taxes to Indirect (that is tax on spending).

This is a means of ensuring revenues - but only where goods and services are bought within the UK. There is a means of identifying imported goods - people make silly mistakes like the pop star who showed off an expensive engagement ring bough in New York and then realised no import duty had been paid on it when she came home. She appears to

have acted in mistaken honesty. Those bringing in cartons of soft drinks openly sold in fast food outlets may not be acting with such innocence.

However, when it comes to services, the situation becomes much more complex. Transfer pricing is, simply, the selling of goods to an overseas company which then resells them at a profit to a domestic purchaser. The cost of R&D is retained in a high tax country (and therefore tax breaks received) but the profit is held in a low tax jurisdiction. For goods, this is reasonably easy to spot. But for services, the physical presence of the provider is not required. Services delivered from cyber-space are intangible. I can easily sell services to a company anywhere world-wide from my PC and a telephone line. I can do this from the top of a mountain in a zero tax economy. Economies which have sold their soul to the devil of the service industry, and to financial services in particular, have to recognise that there is now nothing, technically, to prevent the major banks buying their own island, setting up their own financial services centre and running their own economy. They simply do not need, for much of their international business, to have their profit centres in New York, Frankfurt, London, Hong Kong or Tokyo. They simply need small scale contracting units in those cities, much as they do now in Birmingham or a host of, in banking terms, satellite towns.

Law firms, accountancy practices and others have the same position. Pie in the sky? No. Why else do so many banks register in Delaware and why is Jersey developing Limited Liability Partnership legislation? There are all sorts of excuses but the bottom line is that profits can be retained where the tax burden is lowest and whilst expensed are incurred where they can most mitigate the tax burden.

Electronic cash, stored on a PC or a card can be freely moved across borders using the internet. But this is also a mere development of an existing system. The simplest way of permitting cash movements is to move small amounts at a time, and from within the financial system. This is so easy it is often overlooked. A business with an overseas branch can make inter-account transfers. But even simpler is the purchase of fictitious goods or services using credit card payments: on-line payments of, say, £5000, are quite possible - all someone has to say is that he was paying the bill for expensive hotel accommodation whilst attending a conference.

Moving electronic cash is simpler, still. Indeed the entire mechanism is designed to permit the easy - and free of banking charges - of money. Transfers from one electronic wallet to another are simple and can be done by ordinary telephone as much as by the Internet. Again, the hold the Internet up as an evil which encourages this type of money laundering is fallacious: it is merely a different means of communication for something which is already done by other methods.

Legislators fact the challenge not of creating new offences, in the main, but of controlling their tendency to plug small holes with too large stops, which prove ill fitting and unwieldy and, as a result of this, have their own leaks. Properly considered legislation will reduce the regulatory burden on the Internet, making minor modifications to existing definitions to simply bring new means of transmitting information within the regulatory framework of existing message transmittal.

Conclusions:

It is often claimed that the Internet is an anarchic medium. However, this is not true. The fact is that it is regulated by a sort of self regulation, which does have a great deal of merit.

Legislation could be introduced to deal with certain types of abuse but many types are no different from those which proliferate using other media including print and telephonic. It is questionable whether the Internet should be regarded as a different medium from those of which it is merely a lineal development. Existing rules, such as those relating to sending obscene material through post or telephones can be simply modified, if not already applicable. Indeed, there is an arguable case for amalgamating legislation for post and telecommunications to embrace in a single and simple Act dealing with the transfer of information in any medium save person to person speech.

But in most cases, the avoidance of risk is in the hands of the victim. If anyone suggesting a person spends money hides behind a false address, the target would be an idiot to deal with him. And regulation which stifles the freedom of the many to protect a small number of fools generally becomes a resented law.

DISCLAIMER: It is not claimed that the messages set out below are fraudulent. They are shown as exhibiting certain of the characteristics which are commonplace in fraudulent mailings without representation as to their actual standing or the standing of any person, legal or natural, to whom reference is directly or indirectly made.

APPENDIX A

Return-Path: hotstocks@directform.com

Received: from [38.12.54.88] (helo=ns1.directform.com)

by nemesis.clara.net with smtp (Exim 2.11 #1)

id 10JPep-0001vM-00; Sat, 6 Mar 1999 22:34:57 +0000

Message-ID: <90666.90627@ns1.directform.com>

From: hotstocks@directform.com <hotstocks@directform.com>

Bcc:

Reply-To: hotstocks@directform.com

Subject: Adv: Hot Stocks Newsletter # 2 (87580)

Date: Sat, 06 Mar 1999 16:26:59 -0400 (EDT)

MIME-Version: 1.0

Content-Type: TEXT/PLAIN; charset="US-ASCII"

Content-Transfer-Encoding: 7bit

X-UIDL: 920759699.8783.thanatos.clara.net

X-RCPT: silkscreen

Status: U

Welocme to Hot Stocks Newsletter #2

If you do not wish to read our Hot Stocks Newsletter,
please follow instructions below. Our system is automatic
and you will be unsubscribed to this newsletter.

To be removed from our mailing list, simply reply with "REMOVE"
in the subject. Or reply to mailto:unsubscribe@directform.com.

Visit http://www.directform.com/hotstocks for full details.

Financial Highlights: Triangle Broadcasting, Inc. (OTC BB : GAAY)

"Mark Twain said: "The secret to success is - find out where the
people are going and get there first". We feel that Triangle
Broadcasting, Inc. (OTC BB : GAAY) has followed that adage to a T.

Triangle Broadcasting Company, Inc. (OTC BB : GAAY) is launching
itself to a bright future. They are the first mass media company
to target gays and lesbians on a national level. Successful companies
always take one step at a time so that they never skip over something
important that will haunt them in the future. First, Triangle Broadcasting
Company, Inc. did extensive surveys. They found out what were the
people's preferences. They also figured out what would be the most
strategic way to market their product and what programs would be
received well by both the gay and lesbian communities and the mass
market. They set up their programming and found what cities they
should target first. Triangle Broadcasting Company, Inc. is going
to start in 15 cities. They have chosen 15 cities with large gay
and lesbian populations. After they have gained acceptance in
these markets, they will expand to a national level. They can
already be received by over 10,000 stations in the United States
and Canada. Triangle Broadcasting Company, Inc. will not expand
until they have made a presence in the markets that they are focusing
on.

Triangle Broadcast Company, Inc. hand-picked it's management
infrastructure. They took broadcast executives who had extensive
knowledge about the industry. Gay and lesbian nightclub owners
were brought in to help formulate the programming. Business
advisors help with the complexities of running a business.
And last but not least real estate people help with the
planning of which communities would be their first targets.

After all this was set up they contacted advertising executives

of major companies throughout the United States and Canada. The response was overwhelming. With all the above factors, and the fact that advertisers are already lining up, success is almost inevitable. This is truly an amazing company with nothing but positive opportunities in front of it.

Once again visit http://www.directform.com/hotstocks for full details.

Thank you for reading Hot Stocks Newsletter #2.

Warmest regards,
Staff at Hot Stocks

****** DISCLAIMER ******

This material is being provided by Hot Stocks, a paid public relations company, and is for informational purposes only and is not to be construed as an offer or solicitation of an offer to sell or buy any security. Hot Stocks is an independent electronic publication providing both information and factual analysis on selected companies that in the opinion of Hot Stocks have investment potential. Companies featured by Hot Stocks or company affiliates pay consideration to Hot Stocks for the electronic dissemination of company information. Triangle Broadcasting Company, Inc. has paid a consideration of 500,000 common shares of Triangle Broadcasting Company, Inc. stock to Hot Stocks in conjunction with this company profile. All statements and expressions are the opinion of Hot Stocks. Hot Stocks is not a registered investment advisor or a broker dealer. While it is our goal to locate and research equity investments in micro or small capitalization companies that have the potential for long-term appreciation, investment in the companies reviewed are considered to be high risk and may result in loss of some or all of the investment. The information that Hot Stocks relies on is generally provided by the featured companies and also may include information from outside sources and interviews conducted by Hot Stocks. While Hot Stocks believes all sources of the information to be reliable, Hot Stocks makes no representation or warranty as to the accuracy of the information provided. Investors should not rely solely on the information contained in this publication. Rather, investors should use the information contained in this publication as a starting point for doing additional independent research on the featured companies in order to allow the investor to form his or her own opinion regarding investing in featured companies. Factual statements in this publication are made as of the date stated and are subject to change without notice.

****
96895

::::::::::::::::::::END OF E-MAIL::

WHOIS search result:

Registrant: Direct Form (DIRECTFORM-DOM) 6860 Gulfport Blvd. So. # 284 St. Petersburg, FL 33707 US Domain

Name: DIRECTFORM.COM

Administrative Contact, Technical Contact, Zone Contact: Parker, Charles (CP7439) directform@HOTMAIL.COM 727-376-5011

Billing Contact: Parker, Charles (CP7439) directform@HOTMAIL.COM 727-376-5011

Record last updated on 01-Mar-99.

Database last updated on 8-Mar-99 06:51:56 EST.

Domain servers in listed order: NS1.DIRECTFORM.COM 205.253.134.12

NS2.DIRECTFORM.COM 205.253.134.13

These are the performance figures taken from Yahoo stock service on 8 March:

"GAAY",0.017000,"3/8/1999","2:17PM",+0.003000,0.015000,0.019000,0.014000,2770500

This means that the last trade before the search was done at USD0.017, mid way between bid and offer of USD0.019 and 0.015. The remainder of the figures do not assist at this stage of an investigation.

::Next Message::::::::::::::::::

Return-Path: <info@smart-stocks.com>

Delivered-To: clara.net-racing@silkscreen.clara.net

Received: (qmail 14930 invoked from network); 18 Oct 1998 16:18:07 -0000

Received: from cyber-host.net (HELO mars.your-mail.com) (208.166.8.30)

by mail.clara.net with SMTP; 18 Oct 1998 16:18:07 -0000

From: info@smart-stocks.com

Message-Id: <199810181958.PAA00354@mars.your-mail.com>

To: user@the.internet

Date: Sun, 18 Oct 98 02:02:18 EST

Subject: AD: Smart-Stocks Discovers Emerging Entertainment Company

X-UIDL: 908727490.14954.thanatos.clara.net

X-RCPT: racing

Status: U

This message is sent in compliance of the new e-mail bill: SECTION 301, Paragraph (a)(2)(C) of s. 1618

Sender : Smart-Stocks, P.O. Box 130544, St Paul, MN 55113
Phone : 1-612-646-8174
E-mail : info@smart-stocks.com

To be removed from our mailing list, simply reply with "REMOVE" in the subject.

J.P. Morgan, the world famous banker at the American Bankers Convention in 1903 was asked what was the secret of his success. He replied "Opportunity passed me every single second of my life, but I was perceptive enough to take advantage of these opportunities." The time is always now!

Companies providing live streaming video content such as Broadcast.Com have had valuations as high as one billion dollars. Alternative Entertainment is a live streaming video content provider for Adult related Internet sites. Adult related sites on the Internet are no only profitable but represent the largest segment of E-Commerce and generate 1.2 billion in annual revenues.

Visit http://www.smart-stocks.com for full details.

Alternative Entertainment (OTC BB : BOYS)
Shares Outstanding 3,013,790
Shares Public Float 980,000
Number Sharholders 790
Approved by NASD for Trading October 7, 1998

Visit http://www.smart-stocks.com for full details.

COMPANY OVERVIEW

Alternative Entertainment, Inc. (the "Company") is engaged in the Adult Media and Entertainment Industry. Specifically, the acquisition, development and operation of Upscale Gentlemen's Clubs and advanced on-line media for E-Commerce on Internet Sites. The Company plans a national chain of Upscale Gentlemen's Clubs with the focus on business and professional male patrons. The main floor, which caters to patrons 25 to 39 years of age, will incorporate an evolving theme concept conducive to a "party atmosphere" and will operate under the trade name BOYS TOYS. Private club facilities of the Boardroom Restaurant will target individuals ages 40 to 65 and offer full service dining, an extensive cigar lounge and a vast selection of premium wines and liquor.

The clubs will enable the Company to facilitate onsite film production and live video streaming of the female entertainers as content to the on-line community. Initially the live content will provide revenues via E-Commerce on Company owned Web Sites. Such content will later be repackaged and distributed through Webmasters and individual owners of the 45,000 established Adult Sites on the Internet.

The Company has an extremely strong management team comprised of several

key executives, including the president, of the leading management company within the Gentlemen's Club Industry. The management team has over 100 years of combined knowledge of the Industry.

INDUSTRY HIGHLIGHTS

$4 Billion a year Gentlemen's Club Industry - 25% pretax margins
3,618,000 average yearly revenue per upscale club - $488 sales per sq. ft.
36% of all businessmen entertain their clientele at Gentlemen's Clubs
$1.2 Billion a year Internet Adult Sites - 70% pretax margins
Media content providers are basically non-existent
Consolidation play exists for both segments of the industry

SELECTIVE FINANCIAL HIGHLIGHTS

The Company has internally raised $2,000,000 to date through a combination of equity and convertible debt. The Company has a San Francisco property (15,000 sq. ft.) under construction and an option to purchase two additional clubs.

Once again visit http://www.smart-stocks.com for full details.

--- Disclaimer ---

 This material is being provided by Smart-Stocks, a paid public relations company, and is for informational purposes only and is not to be construed as an offer or solicitation of an offer to sell or buy any security. Smart-Stocks is an independent electronic publication providing both information and factual analysis on selected companies that in the opinion of Smart-Stocks have investment potential. Companies featured by Smart-Stocks or company affiliates pay consideration to Smart-Stocks for the electronic dissemination of company information. Alternative Entertainment Inc., has paid a consideration of 5,000 common shares of Alternative Entertainment Inc., stock to Smart-Stocks in conjunction with this company profile. All statements and expressions are the opinion of Smart-Stocks. Smart-Stocks is not a registered investment advisor or a broker dealer. While it is our goal to locate and research equity investments in micro or small capitalization companies that have the potential for long-term appreciation, investment in the companies reviewed are considered to be high risk and may result in loss of some or all of the investment. The information that Smart-Stocks relies on is generally provided by the featured companies and also may include information from outside sources and interviews conducted by Smart-Stocks. While Smart-Stocks believes all sources of the information to be reliable, Smart-Stocks makes no representation or warranty as to the accuracy of the information provided. Investors should not rely solely on the information contained in this publication. Rather, investors should use the information contained in this publication as a starting point for doing additional independent research on the featured companies in order to allow

the investor to form his or her own opinion regarding investing in featured companies. This publication contains forward looking statements that are subject to risk and uncertainties that could cause results to differ materially from those set forth in the forward-looking statements. These forward-looking statements represent Alternative Entertainment Inc., judgement as of the date of this release. The company disclaims any intent or obligation to update these forward-looking statements. Factual statements in this publication are made as of the date stated and are subject to change without notice.

Whois Query Results

```
No match for "WWW.SMART-STOCKS.COM".
```

Note the close similarity between the style and wording of these two documents. Note also that WHOIS returns on 8 March a no match for the domain name that asks you to invest your money.

::