

BRITISH BROADCASTING CORPORATION

RADIO 4

TRANSCRIPT OF "FILE ON 4" - "FINANCIAL WAR ON TERROR"

CURRENT AFFAIRS GROUP

TRANSMISSION: Tuesday 3 June 2008 2000 - 2040

REPEAT: Sunday 8 June 2008 1700 - 1740

REPORTER: Fran Abrams

PRODUCER: Rob Cave

EDITOR: David Ross

PROGRAMME NUMBER: 08VQ4263LH0

THE ATTACHED TRANSCRIPT WAS TYPED FROM A RECORDING AND NOT COPIED FROM AN ORIGINAL SCRIPT. BECAUSE OF THE RISK OF MISHEARING AND THE DIFFICULTY IN SOME CASES OF IDENTIFYING INDIVIDUAL SPEAKERS, THE BBC CANNOT VOUCH FOR ITS COMPLETE ACCURACY.

“FILE ON 4”

Transmission: Tuesday 3 June 2008

Repeat: Sunday 8 June 2008

Producer: Rob Cave

Reporter: Fran Abrams

Editor: David Ross

ABRAMS: This month the world’s experts on terrorist funding will gather in London. For the past year, Britain's been leading the international task force on the issue. Ministers have underscored the importance of clamping down on Jihadi money.

EXTRACT FROM GORDON BROWN SPEECH

BROWN: Ladies and gentlemen, there should be no safe haven in the world for terrorists and there should be no hiding place anywhere for those who finance terrorism. And what I want to announce today is the framework of a new regime we’re developing nationally and internationally for rooting out terrorist finance.

ABRAMS: The Government says its policies have been a success. But if that’s the case, why are thirteen suspected terrorists running UK companies? And what about the London bank accused by the US of channelling funds to Hezbollah? Why has it never had a visit from our Government inspectors? Are we really winning the financial war on terror?

SIGNATURE TUNE

ACTUALITY OF TSOULI WEBSITE

ABRAMS: This is a website with instructions on how to make a suicide vest. These DIY guides to bomb-making are widely available on the internet.

ACTUALITY MUSIC & BANG

ABRAMS: This one was found on the computer of a cyber-terrorist known as Irhabi - or Terrorist - 007.

KOHLMAN: When Al-Qaeda in Iraq wanted to release a new video of a beheading or a new video of a suicide bombing, the video would actually be released through Irhabi 007. He was essential in the distribution and creation of Al-Qaeda propaganda, not just actually, you know, spreading it around to the world, not just uploading to internet sites. He set up an entire communications network, an internal communications network for these people.

ABRAMS: Security services across the world wanted to find Irhabi 007. One of those on his trail was Jihadi website watcher, Evan Kohlman.

KOHLMAN: Well, it was quite clear that he was located in Europe. He was obviously quite fluent in English. I actually at one point corresponded with him in English over email. He didn't write to me in Arabic, he didn't write with traditional Islamic salutations. He wrote, "Dear Evan". He was a very westernised individual and it was quite clear from everything that he did that he was living in a major city in a westernised country, and the assumption always was the United Kingdom, it was always London most likely, but for a while he did a fairly good job of covering his tracks.

ABRAMS: Despite all the attention Irhabi 007 was attracting, no-one could actually track him down. Then, in October 2005, a potential suicide bomber called Mirsad Bektasevic was arrested in Bosnia. In his flat, police found a video proclaiming his desire to become a martyr for Islam. And on his phone they found a recent call to someone in London.

ACTUALITY IN SHEPHERDS BUSH

ABRAMS: Within three days the police were breaking down a front door in this scruffy side street in Shepherds Bush, West London. They were in luck. Inside they found Irhabi 007, who was actually a 19 year-old Moroccan man called Youness Tsouli. When the police arrived, he was building a website called “You Bombit.” And the trail didn’t stop there.

The police quickly linked Tsouli to another man, Tariq Al-Daour, who lived about a mile away in Bayswater. At his house they found two computer memory sticks containing some startling information - details of no fewer than 37,000 stolen credit cards.

KOHLMAN: What you had was one of Irhabi 007’s associates on the internet, an individual by the name of Tariq Al-Daour and who had actually never met Tsouli – Irhabi 007 aside from online, they’d never actually met in person. However, Al-Daour, from the age of fifteen, had become very very proficient at internet fraud techniques, expert at stealing credit card numbers – and not just stealing the credit card numbers themselves, but by creating complete profiles of the victims - their names, their addresses, their Social Security numbers, which would allow a potential scam artist to really get the most out of these cards. And essentially what he would do then is take the proceeds and launder it using internet gambling sites, again all using stolen credit card numbers. And as Al-Daour became more and more wrapped up with Irhabi 007, with Youness Tsouli in this Jihad on the internet, more and more of these techniques that had been honing since the age of fifteen came into play.

ABRAMS: How much money did Al-Daour make from these scams and what was done with the money?

KOHLMAN: Well, I mean, in total the amount was in the millions of dollars. Some of this money was used to purchase goods, electronic equipment, etc. These credit cards were also used for another very important purpose, which is that essentially in order to register a website on the internet you basically have to have a credit card, and that makes it very difficult for organisations like Al Qaeda to set up a major permanent internet presence. So the solution that Al-Daour and Irhabi came up with was that they were using these stolen credit cards in order to register dot com websites.

ABRAMS: The fraud amounted to £1.8 million. Tsouli was jailed for ten years and Al-Daour for six and a half. But the pair had operated for between two and three years before they were caught. The Metropolitan Police won't talk publicly about the case, but we understand they believe Tsouli had a direct link to Al-Qaeda. Online fraud is a huge and growing area, costing the UK around £300 million a year. In this great sea of crime, it can be hard to pinpoint the most serious or even dangerous offenders.

ACTUALITY WITH COMPUTER

GOODWILL: So if you look at that transaction, those are the details of the card there. So if you click on the card, that'll actually tell me who the rightful owner is, because that's clean data. That's why I was saying she lives in Kettering but he's using it, that one's false, that one's also false.

ABRAMS: Andrew Goodwill's interrogating an anti-fraud database he keeps for the online retailers. This system stores all our transactions, so if our spending patterns change, a possible fraud can be highlighted.

GOODWILL: So when you actually look at that address, you will see that there are 183 transactions.

ABRAMS: And Mr Goodwill says it could have picked up the fraud Mr Al-Daour was committing.

GOODWILL: If that happened today, our analysts would be picking that up very very quickly because internet retailers would be telling us that they had received orders from a specific address using lots of different card numbers, and that for us would start to ring bells – not necessarily that Mr Al-Daour was a terrorist or that he was a criminal in any way whatsoever. We would pick up the suspicion that something was happening at that particular address that was out of the ordinary and for us that would give us a direct suspicion that fraud was taking place.

ABRAMS: Does it surprise you the police only picked that up by chance?

GOODWILL: It doesn't actually because it would be very difficult for a bank or a financial institution or law enforcement to actually pick that information up. What we have is retailers' data – so that's internet retailers' information about a transaction. A bank don't store that information.

ABRAMS: Do the police have access to this information?

GOODWILL: They do, but on an informal basis at the moment. We are looking at trying to set up some formal systems so that they can have access to this information, but at the moment it's done informally and we will actively work with the police wherever possible.

ABRAMS: And the police have other obstacles in their path too. We've discovered even cards that have been cancelled abroad can be used here – and big criminal operations are aware of that. Mike Harris of the Lothian and Borders Police in Scotland, has investigated a large number of credit card frauds, including ones with terrorist links. He says that loophole's been exploited.

HARRIS: We did investigate one from 2003 through to 2006 which did result in the conviction of individuals in this country who had been receiving what we call bust out cards from the US, which are accounts that are opened in the US using false details and false addresses, building up their credit rating and then absolutely hammering the card, taking as much money and goods out as possible. And when the bank company went to look for the individuals, there was nobody there, so they then killed the card dead in the US. The cards were then sent in a package over to the UK, and so long as they're kept below the floor limit in the UK, the cards could continue to be used, and all that happened was it was repeated in the UK at a lower level and the funds were then sent back to a central point. We had funds going back to Pakistan, we had funds going out of the country to the near continent in Europe, and we had funds that were just to-ing and fro-ing in British bank accounts and then off out to the States again.

ABRAMS: How did that eventually get picked up then, and how long did it take?

HARRIS: It got picked up by one individual in American Express, who became aware of one name coming up several times and tried several different police forces throughout the UK, tried to get them interested in it and eventually came into our force up in Scotland.

ABRAMS: The total fraud added up to £6 million. Mike Harris feels there was a risk the money could have been going to fund terrorism. One key sign was that the lifestyles of the perpetrators were far from lavish - and the money had all been shipped abroad.

HARRIS: What we get are the foot soldiers who are never usually involved in any other sort of crime, they have never come to the notice of the police for any other reason, they don't try to draw any attention to themselves, and they live a fairly meagre lifestyle, and no trappings of wealth which obviously meant that they were not receiving the full proceeds of what they were carrying out and that the funds were going elsewhere. What they were doing was handing the money over to the middleman and they didn't know what happened thereafter.

ABRAMS: What does that indicate to you about the type of operation it was?

HARRIS: Obviously there is obviously a structure to it in that the fact of the matter is, what is the money going to? I mean, it could have just been organised crime, it could have been that there was somebody back, say, in, as I say, a lot of the funds went back to Pakistan. There could be somebody sat back in Pakistan with a very large amount of money or owning a lot of land, but it's very difficult to trace funds once they go back to somewhere like that, because we don't have specific bank account details.

ABRAMS: How easy is it for you to pick that up when somebody's doing this kind of thing?

HARRIS: In our force, we have round about ten officers who are dedicated to fraud, that's not specifically credit card fraud, that's every sort of fraud.

ABRAMS: Is that enough?

HARRIS: Personally I don't think it is, but there again, to use an old adage, fraud is not sexy. It takes a lot to look beyond what the fraud is actually there for. The fraud is used, as we say, for terrorism, it could be used for funding drugs operations, it could be used for organised criminal gangs to move people about, people trafficking. A lot of the time, the actual funding aspect of it is overlooked by the hierarchy in both the police and perhaps in Government, and it's looked at as more a case of, ah well, that's just the financial institutions that are losing out, it's not harming any one individual.

ABRAMS: According to the US Jihad-watcher, Evan Kohlman, there are even manuals now to explain the basics of becoming a cyber terrorist. He says we should expect to see more of this type of thing.

KOHLMAN: Large scale financial fraud, particularly identity fraud and credit fraud, are indeed a major trend in terms of where Al Qaeda and other groups are headed for financing, and it's very easy to understand. The traditional methods that Al Qaeda and other terrorist groups have used to finance themselves, individual donors, Islamic charities, whatnot, there has been a major crackdown on this sort of activity in the last eight years. So in other words what's happened is that terrorist financing has had to really shift, and it's also shifted because now you see out there the rise of homegrown terrorism. They are having to fund themselves, and when it comes to small time Jihadis or homegrown Jihadis, who are very technologically skilled, it's really only natural that they would turn to the internet in order to fund their ventures.

ABRAMS: In the UK, the responsibility for terror financing rests with the Treasury. During the making of this programme we asked repeatedly to talk to the responsible minister, Kitty Ussher. Among the questions we wanted to ask was whether the police had sufficient powers to tackle this kind of cyber fraud. But the Treasury refused to make any minister available. In response to our written questions, they issued a statement.

READER IN STUDIO: The UK has strong legal foundations to support action against computer-related fraud. A new National Strategic Fraud Authority is now being created to strengthen the national response to fraud and is adopting 'e-crime' as an early priority.

ABRAMS: While it may be difficult for the police to pinpoint the most serious kinds of credit card fraud, sometimes an allegation is crystal clear - and yet the Government doesn't seem inclined to act.

ACTUALITY OUTSIDE SADERAT

ABRAMS: We're right at the heart of the City of London. In fact, we're just one street away from the Bank of England, and I'm standing outside the London office of Saderat, which is an Iranian state-owned bank. The US Government claims that between 2001 and 2006, Saderat channelled money to the proscribed group Hizbollah through this branch. Yet while the American authorities have taken action against the bank, here it's still open for business.

The sum alleged by the US Treasury to have passed through London to the militant Lebanese group was approaching £30 million. That department's Assistant Secretary, Pat O'Brien, says it had no choice but to apply sanctions, to stop the bank doing business internationally.

O'BRIEN: We took action against bank Saderat in September 06 and then subsequently we later designated them under our terrorist financing authority. Iran used the state-owned bank as a conduit for providing funds to a variety of terrorist organisations, including Hizbollah and Hamas and Palestinian Islamic Jihad, and in the Saderat case we saw money go from the Central Bank of Iran through Saderat to Lebanon to these various terrorist organisations in very substantial amounts of money, you know, multiples of millions.

ABRAMS: What would you like the UK to do about the continued existence of Bank Saderat in London?

O'BRIEN: Ultimately I would say that's a decision for the UK to take based on the authorities and the rules and regulations that they have in place here in the UK, so obviously we want all jurisdictions to do as much as they can under their national authorities to control the activities of these banks.

ABRAMS: He's being very cautious. His boss is on record as expressing disappointment that there hasn't been swift action in Europe. The Financial Services Authority's supposed to investigate if there's a risk a crime's been committed by a bank. And indeed, Bank Saderat told us not only would it be happy see the FSA, it actually invited them in, in the hope of clearing its name, but the inspectors never visited. The bank says its audit reports confirm its innocence.

READER IN STUDIO: We have made every effort ourselves to obtain details of the alleged evidence against us. It is highly regrettable that we have had no opportunity to defend our position, and it is equally regrettable that the UK Government appears not to have considered it appropriate to obtain and assess evidence from the US Treasury.

ABRAMS: We asked the FSA several times to tell us what, if not this, would spark an inquiry by its officials. It refused to comment on why it hadn't interviewed Bank Saderat about the allegations – but it did add such decisions were made on a case by case basis. The UK's been discussing the Iranian banks with its European allies. There are others which have been accused of supporting Iran's nuclear programme. But the shadow Foreign Secretary, William Hague, thinks Britain should act alone if necessary. And he's puzzled about the role of the FSA.

HAGUE: Where there is any uncertainty or allegations, one would imagine that the Financial Services Authority would investigate, and over time we will want to know what they have done about it. I don't think we would expect them to give a running commentary on these things, but we will want to know whether all of these accusations, allegations have been properly investigated in due course.

ABRAMS: Do you get the impression that the British Government is pushing this vigorously?

HAGUE: Well, I had the impression that they, like me, want to see European action against Iranian banks, but I certainly have the impression that they haven't secured agreement for that. It's high time that it was agreed, and we have asked the Government on several occasions in recent months in the House of Commons whether this

LEPPAN: Well, it's relatively simple. We need to be raising the barriers on who can register as a UK company directory. This isn't rocket science, in the same way that we would not want to be issuing a visa or permitting somebody to board a plane or to immigrate if they had very strong terrorist ties. We equally should be requiring that when it comes to registering a UK company.

ABRAMS: The thirteen alleged terrorists found by Worldcheck on the Companies House register included one who'd been convicted of selling false passports and another who was on an official sanctions list. Baroness Pauline Neville-Jones, former head of the Joint Intelligence Committee and now Shadow Security Minister, believes regulation of companies should be tighter.

NEVILLE-JONES: I'm not entirely clear, you know, what the Companies House does when it receives a registration of someone. It is very clear under law that you have to be a fit and proper person, pretty much by definition, if you were associated with any kind of terrorist financing or indeed any kind of activity of that nature, you would not qualify for being a fit and proper person. So I suspect that the role of Companies House is more passive than probably it should be now. What hasn't happened, I think, in all of this legislation is that at no point has anybody taken the whole body of it and said, where do we need to try and put in the barriers that will really trap the improper activity without impeding what is legitimate.

ABRAMS: We asked Companies House to talk to us about what it does to ensure directors are 'fit and proper' persons. It directed us to its parent department: the Department for Business, Enterprise and Regulatory Reform. They referred us to the Treasury, which oversees policy on terrorist financing. And they declined to give us an interview. But they did give us a written statement.

READER IN STUDIO: We have reviewed whether Companies House is open to terrorist exploitation, and concluded that Companies House rules do not pose any vulnerability of terrorist abuse of the financial system.

ABRAMS: So, there's a lot the Government isn't doing. But there's one area where there's been a great deal happening – the banking sector. Its been through a big reform to ensure all suspicious activity is picked up and the police are told about it.

ACTUALITY OF SIRENS & SHOUTING FROM 7/7

MAN: Move away from this road please!

WOMAN: You could hear the screaming from the carriages in front, because that was where the explosion had happened.

MAN 2: Our carriage was smoke-filled, there was lots of dust, there was lots of panic. We could see the people covered in blood.

ABRAMS: On the morning of July 7, 2005, four young men alighted here at Kings Cross station from a Luton train. They embraced and went their separate ways. Nineteen year-old Jermaine Lindsay boarded a Southbound Piccadilly Line train – and in its first carriage he detonated his bomb, seventy feet underground. The blast from Lindsay's rucksack killed twenty-six other people and left more than three hundred and forty injured. In total, the bombings left fifty-two innocent people dead. Within hours, the police were starting to follow the money trail.

DILLOWAY: I was given the job of costing the attack by means of finding out how much all the components had cost and all the other expenses involved in putting the attack together, and also of trying to establish where the funding had come from. And it was things like bits of credit cards and bank cards which assisted the unit to identify who the bombers were within a very short space of time.

ABRAMS: Simon Dilloway was a team leader in the Metropolitan Police's specialist terror finance team. He had a painstaking job to do.

DILLOWAY: I was provided with the scenes of crime photographs and my job on that particular occasion was to collate all the different items there, identify what they were and then establishing an estimate of how much that would cost.

ABRAMS: What did you find out?

DILLOWAY: Well, I found out that in fact the amount needed to actually carry out this attack was surprisingly small. If you looked just at the materials that were actually used, the cost of transportation for purchasing certain of the more exotic items and car hire, train tickets, the sum is no more than £2,500. When you add in things like costs involved in recruiting campaigns and travelling to Pakistan for training, as was suspected, the maximum that we could get it to come to was a little under £7,500.

ABRAMS: The bombers had raised the money in surprisingly mundane ways – mostly loans and credit cards. There is a system that's supposed to pick this sort of thing up. Banks are meant to tell the police if they spot anything that might indicate terrorist financing. They do it under something called the Suspicious Activity Reports Regime, or SARS. And indeed, official accounts later confirmed Jermaine Lindsay's bank had picked up a change in his behaviour.

READER IN STUDIO: Lindsay made a number of purchases with cheques (which subsequently bounced) in the weeks before the 7 July. Bank investigators visited his house on the day after the bombings. Although Lindsay was not specifically identified as a terrorist until after an attack took place, this case demonstrates that financial intelligence was sufficiently accurate to prompt investigation by financial institutions.

ABRAMS: That was a report from the financial action task force – the body that sets international policy on terrorist financing and of which Britain's held the presidency for the past year. And it seems to indicate the system worked. But while Lindsay's bank had employed some private investigators to ask why his cheques had been bouncing, according to Simon Dilloway, that hadn't been enough to spark a formal report under the SARS system.

What information was there on the SARS database about the bombers?

DILLOWAY: To my recollection there was no significant information on these particular people, but then again the financial activity was at a very low level, the majority of them only used cash that they withdrew from their benefit payments or whatever low paid jobs they had at the time, so there was very little opportunity for them to actually

ABRAMS: We've been told there were no SARS on the bombers and that furthermore, you know, that system, the SARS system could never even be expected to detect such small things as bouncing cheques or unpaid personal loans, which is what had gone on.

ARMOND: I think that question arises from a fundamental misunderstanding of what SARS are supposed to be about. The whole purpose of the SARS regime in relation to terrorism is to allow investigators firstly to look backwards by piecing together how a criminal or terrorist conspiracy was developed and the timelines involved. Secondly, to enable them to look sideways by identifying or confirming associations between individuals and activities. And finally it enables investigators to look forward by identifying warning signs of criminal or terrorist activity in preparation.

ABRAMS: We've interviewed one of the investigators who did that report into the 7/7 bombings. He says that the SARS system could never be used or is very unlikely to be used to prevent a domestic terrorist attack. Is that right?

ARMOND: What I've said to you is that the SARS database has been useful in all of the elements that I've suggested by looking backwards, sideways and forwards in time, by investigators in relation to terrorism matters, so I'd have to take issue with whoever it is you've spoken to. What I am saying to you is that since that time, there are examples where the SARS database has proved to be useful within this context.

ABRAMS: In preventing attacks rather than looking at what's happened after the event?

ARMOND: You don't seem to be listening to me. In relation to all three elements, so that's particularly by looking backwards when conducting an investigation, by looking for associations and links, and also by identifying warning signs of criminal or terrorist activity and preparation.

ABRAMS: This suspicious activity regime's been beset by other problems too. Two years ago, an official review by Sir Stephen Lander warned it needed a major overhaul. A key recommendation was that the computer that runs the SARS database

ABRAMS cont: system needed upgrading. He suggested it might take a couple of years and cost around £5 million. Baroness Neville-Jones, the shadow security minister, says although the database now holds more than a million suspicious activity reports, it still isn't working properly.

NEVILLE-JONES: One gets hints. I have to say they're hints because we are not properly informed about SOCA. It's one of the problems, I think, that their IT is not as good as it might be and could be, and of course it may be expensive to fix. You can pour a lot of information into a system, but if that system is not capable of retrieving it under a large number of headings - ie it's not filed sufficiently flexibly, to put it in simple terms, you're not then necessarily going to be able to get out of your system the information that it actually contains, and I suspect, but I don't know, that is one of the problems.

ABRAMS: And of course it's two years now since SOCA was set up with a very clear aim to upgrade its systems. What do we know about where they're up to?

NEVILLE-JONES: One certainly gets the feeling that actually the current head of it feels that one of his problems is that his own recommendations weren't implemented when he came in to office. I suspect that on the ministerial side they feel that the record of the agency is so poor, they are very chary about pouring more money in, and I suspect you've got both of these problems operating, and the net result, as I've just said, is a very low level of performance.

ABRAMS: SOCA's now talking not just about improvements to its SARS database but about a £50 million overhaul of all its IT systems - something it says is about to go out to tender. The agency's deputy director, David Armond, says this is in line with what was recommended in Sir Stephen's review.

It's more than two years now, isn't it, since Stephen Lander said that the information technology wasn't being used properly and needed upgrading. Has that happened?

ARMOND: There have been significant improvements both in terms of the systems that we are using, the IT that we are using and also the fact that all the material is now directly accessible by 75 law enforcement agencies.

ABRAMS: That doesn't sound like the recommendation was met then? You say you haven't even gone out to tender yet.

ARMOND: That's not what I'm saying at all. There were twenty-four recommendations. Part of one of the recommendations related to a completely new IT system, and obviously that will take some time to deliver, but the rest of the recommendations have been met.

ABRAMS: Stephen Landers seemed to envisage that would take place within a couple of years, didn't he? He said £3 million the first year, a couple of million pounds the next year and then just refreshment. He seemed to think it would be done by now.

ARMOND: As you well know, this is eighteen months into significant developments in relation to the IT process, and this is completely in accordance with the time scales that we estimated for delivery.

ABRAMS: So if we come back to you next year we'll find that all the systems, the new systems are in place, will we?

ARMOND: Now that's not what I've said at all. This could take some time to roll out. But we are in the process of going to tender for some new IT equipment which will deliver further improvements to the system.

ABRAMS: But there are wider questions about SOCA's role. It was supposed to be Britain's FBI, with a wide-ranging brief to stop major criminal gangs in their tracks. But Jonathan Fisher, a QC specialising in fraud and a visiting professor at the London School of Economics, thinks the agency's taken a wrong turn. He fears it's more interested in patterns of crime than in actually catching criminals.

FISHER: As I understand it, what SOCA want to do is move onto a much more generic system whereby the information will come in and, instead of focusing on the precise nature of the of the criminal activity, what they would like to do is use the information in a much broader and generic sense to build a picture of what type of criminal activity is occurring in the country.

ABRAMS: So what would be the impact of that on SOCA's ability to catch criminals?

FISHER: Well, in one sense of course, you could argue that it might limit the ability. The problem with terrorist financing is that one is looking for a needle in a haystack. And my concern is that by switching the emphasis from something that is specific to something that is more generic, the ability to identify people involved in terrorist financing will be diminished. And therefore I think that they're going to have to go back and use good old fashioned intelligence techniques to penetrate the terrorist cells and to build up their picture in that way.

ABRAMS: But there may be a problem with that. Although SOCA runs the suspicious activity reports database, it isn't actually responsible for tackling terrorism. If it spots a terrorist network moving money around, it has to pass that information to the Metropolitan Police. But David Armond, deputy director of SOCA, doesn't agree with the agency's critics. He rejects the claim that it's more interested in trends than crime.

ARMOND: That's absolute and complete nonsense. It's SOCA's job to pull together all the information and to disseminate it to the relevant agencies. And in relation to terrorist finance, these matters are referred directly to the Metropolitan Police service.

ABRAMS: So you don't actually investigate terrorist crime then? You pass on reports, basically?

ARMOND: No, we provide reports, we are the gateway for reports which come from the regulated sector, and we provide operational support in certain circumstances. Some Suspicious Activity Reports are in themselves a golden nugget for an investigation. Quite often it's the information that is obtained within them – things like names, addresses, dates of birth, associations and the like, bank account details when linked to either other SARS within the database or to other datasets that we've got. That's when the useful leads come in.

ABRAMS: Baroness Neville-Jones said she suspects ministers don't actually have enough confidence in the way SOCA is being run and said they don't want to put more money in.

ARMOND: I think that's entirely unfair and that's not the case at all and we're quite content with the settlement that we've been given this year.

ABRAMS: The SARS system's just one plank in the UK's strategy for tackling terrorist finance. But with little emphasis on company rules, a lack of vigilance when it comes to regulating banks and a huge rise each year in internet fraud, is there is a risk we could lose ground on this vital front in the war on terror? In its statement, the Treasury was upbeat.

READER IN STUDIO: We have a robust and effective counter terrorist finance regime that deters, detects and disrupts the financing of terrorism in an effective and proportionate way. The Financial Action Task Force evaluated the UK's Money Laundering and Terrorist Finance controls last year, and judged the UK's anti terrorist finance regime to be among the best in the world.

ABRAMS: As a key ally of the US, Britain has made serious efforts to ensure its systems aren't abused. But three years after the July 7 bombings, the shadow Foreign Secretary, William Hague, says there's no room for complacency.

HAGUE: Well, there is a huge threat from terrorism internationally, it hasn't gone away, people relax a little once terrorism outrages fade from the news, but clearly there is a major terrorist threat, including to this country, and it's very important that we do everything possible to stop the financial system being abused in a way which helps terrorism. So we have to be vigilant about terrorist financing in general. I hope that no one in Government is complacent about it, but it is very important that we continue to intensify our efforts.

SIGNATURE TUNE