## Information Sharing – Light from the Black Hole?

*The regulated sector has to commit much in the way of resources to compliance, but many firms have been complaining that the information flow is one way, and that they never see the results of their efforts. How is that being resolved in the UK?*

The various anti-money laundering statutes and regulations of recent years have included a significant aim – to wrest information from the regulated (primarily financial) sector, to assist in the fight against crime, money laundering & terrorism. By making use of the interface between the public and the established financial systems, much has been done to make life difficult for those who are intent on committing financial crime, and abusing those systems. The Suspicion Reporting Regimes that have evolved in the UK are responsible for making available large amounts of intelligence, irrespective of whether or not they have led directly to prosecutions, or even investigations.

The 3rd EU Money Laundering Directive, which is almost entirely enshrined in United Kingdom law by the Money Laundering Regulations 2007, encourages member states to lean towards the reporting of suspicious *activity* rather than *transactions*, an approach already adopted by the UK. Suspicious Transaction Reporting (STR) generally involves the use of reporting thresholds, and/or concentration on the actual transaction - origin, destination, method (cash etc). This approach is inefficient for a number of reasons. Thresholds merely induce launderers to ensure that they enter the markets below the stated level, and spread their forays among different service providers.

It also means that many reports are made unnecessarily, because they are in no way actually suspicious, just big, and a lot of time is wasted. Focussing on the single transactions, rather than the bigger picture of the actual activity of the customer, may conversely mean that some transactions that do not appear suspicious in themselves get ignored, while they are actually significant within a pattern of behaviour which should arouse suspicion.

The greater efficiency of the Suspicious Activity Report (SAR) regimes, where the transaction, the account activity, and the account holder are all considered together, is difficult to deny. The added imperative of the Directive and the 2007 Regulations to apply a *Risk Based Approach* (RBA) to due diligence and account monitoring activity means that even more reports are made by staff and compliance officers adopting a 'belt and braces' approach, or perhaps, more cynically, covering their backs against the possibility of prosecution for failing to report activity to the UK authorities.

The overall consequence of these developments is that there is a whole lot of data held by the Financial Intelligence Units (FIU). The United Kingdom FIU, housed at the Serious Organised Crime Agency (SOCA) in London, received over 220,000 SARs between October 2006 and September 2007 *(The Suspicious Activity Reports Regime Annual Review 2007:SOCA).* These reports were then evaluated, first by digital methods, then if of concern, by trained staff, and entered onto the FIU database. Those disclosing information in key areas, such as Terrorism and Corruption, were sent directly to the appropriate specialist police units, whilst the rest were made available for investigation by accredited officers in forces and other agencies around the country that have access to the database.

The benefit of this system is that the reports containing genuinely suspicious activity can be appropriately dealt with. It also means that there is a lot of other intelligence available for interrogation when required; intelligence that may provide invaluable evidence of associations between suspects under investigation, or in the aftermath of a terrorist incident. The database thus has both a pro-active and a re-active function. Its very presence, as a repository of SARs, themselves a serious obstacle in the path of the financial criminal of whatever shade, is a deterrent, or at least cause for thought.

Its *raison d'être* is to identify criminal behaviour in those dealing with criminal property, and many investigations have been initiated by SARs. The reactive function occurs when financial investigators run details of their suspects and associates through it, and important details provided by the suspects as customers of the regulated firms can be obtained. The database, know as ELMER, is regularly interrogated by investigators dealing with the serious conventional crimes as well as terrorism.

It is not a perfect tool, however, and like most tools, care must be taken to use it properly. Various reports have been made, most notably on the Financial Action Task Force (FATF/GAFI) website, that SARs contributed to the identification of one of the suicide bombers who attacked London in July 2005, Jermaine Lindsay. That claim was incorrect, as no SAR had been submitted, and the action described was normal bank investigation of the running up of unauthorised debt on an account. In actual fact, none of the financial behaviour of any of those involved in the attack could in any way be expected to find its way into a SAR. The amounts were minimal, and the behaviour not unusual for young men in their circumstances. The regime is not at fault in this situation, it should not be expected to perform this function, and it is important to understand that it does not *(note to editor: I investigated the costing and funding of the attack whilst in the National Terrorist Financial Investigation Unit, and produced the report for the UK Govt on its implications)*.

So how does all this address our original question? It can be seen that the system that has developed in the UK is functioning reasonably well from a law enforcement point of view, which is what it is there for. The raw material for this function, however, comes not from law-enforcement, nor from the government, but from the private sector – financial institutions, insurance companies, lawyers, casinos, accountants, real-estate agents, etc., etc. The response from the sector has been variable, and it would be fair to say that co-operation has increased in line with the increase in legislation forcing co-operation!

This should be no surprise, as complying with the law often means loss of business, and it certainly means increased staffing and infrastructure costs. Companies often say, frequently in their statement of ethical behaviour, that they would not wish to do business with criminals, and this legislation helps them to fulfil that wish. To be fair, however, a great but necessary burden has been placed upon the regulated sector, and the most common complaint heard at any gathering of compliance officers is that of the 'Black Hole'; the black hole where all of the information and reports go when they submit them, never to be seen or heard of again.

It might be said that it is of no concern of the banks and others what happens to that information once submitted; it is a valid point, especially when weighed against the anonymity guaranteed to the maker of the report by the legislation. However, the essence of the complaint is not really some prurient desire to find out what happened, but more to get some feedback as to actually what is or is not useful for the effective prevention and detection of crime and terrorism. The suspicion and risk based approach of the system means that no definition is given of what should or should not be reported; so, the regulated sector says, any feedback would help to direct their efforts in the most efficient way.

Providing some feedback to the sector in an informal way has been done for some years now by the police. Following the excellent response by the financial sector to the suicide attacks on London in 2005, its representatives were invited to seminars by the National Terrorist Financial Investigation Unit. They were given an indication of how their contribution assisted in the post-incident investigation and other ongoing operations. This was not entirely, or even mainly, about the SAR regime, however it gave information (albeit limited, owing to the sensitivity of the subject) back to the financial sector, and helped those employed in it to see some of the results of their efforts.

On a wider scale, and specifically in the SAR arena, sections 33 & 34 of the Serious Organised Crime & Police Act 2005 developed a system of 'gateways' through which information could be shared with anyone that SOCA thought appropriate. There have also been developed a system of 'Alerts' to highlight particular issues or vulnerabilities to the FIU information providers. These Alerts are formulated by the 'Vetted Group', made up of Law-Enforcement officers together with members of the industry who have been vetted, or security screened, to a very high standard. This enables a two way flow of information, and a mutual understanding of the problems facing both the suppliers and receivers of information in the form of SARs. There have also been around 200 seminars and bi-lateral visits annually run by the FIU with the financial sector.

Whether or not the industry feels that these efforts are addressing their previous complaints, whether there is light escaping from the 'Black Hole', is difficult to judge – certainly the SARS annual report 2007 contains endorsements from private sector members, but only time will tell how effective that these initiatives have been.

What is difficult to deny is that the judicious use of information-sharing is mutually beneficial wherever it is attempted. When one understands the motivations, the rationale and the obligations of the other party in a situation of mutual interdependence, there grows an appreciation of each other's problems, and a united effort can be made to solve them. It is to be hoped that the initiatives taken in the UK do produce results, and are given an opportunity to develop and expand. It is a model that others, both nationally and internationally, would do well to emulate.

(1622 words)

**Simon Dilloway** ***BSc(Hons), MSc, MSyI***
***Principal***
**Lopham Consultancy**
**+44 (0)1379 687593**
**+44 (0)7815 300169**
**sdilloway@lophamconsultancy.co.uk**
**www.lophamconsultancy.co.uk**