

TECH 07/06

**THE CONFIDENTIALITY OF MONEY LAUNDERING SUSPICIOUS
ACTIVITY REPORTS (SARs) IN THE UNITED KINGDOM**

Technical Release issued in September 2006, analysing the current situation in England and Wales, on the reporting of money laundering and terrorist financing, in relation to prevention of the disclosure of the identity of reporters to suspects or their representatives.

Contents

Introduction	1 - 5
Government Policy on the Confidentiality of SARs	6 - 11
Disclosure required by Law	12 - 13
Disclosure by a Law Enforcement Authority not covered by Home Office Guidance	14 - 17
Corrupt or Criminal Disclosure	18
Disclosure due to administrative error	19 - 20
Disclosure under the Freedom of Information Act	21 - 22
Disclosure under a Subject Access Request under the Data Protection Act.	23 - 25
Implications for Civil Cases	26
Self Help	27 - 29
Conclusion	30 - 31

INTRODUCTION

1. Continuing concern has been expressed by office holders and members, about the confidentiality of SARs, some of which concern is undoubtedly justified. This is an issue which has already been the subject of sustained lobbying by the accountancy sector representative (the Chairman of the ICAEW working party) through the medium of HM Treasury's Money Laundering Advisory Committee (MLAC) Reporting and Feedback Working Group. This lobbying is in co-operation with the Law Society, BBA and ABI representatives, as this is an issue of concern for the whole regulated sector, and one which particularly the Banks have been struggling with for years. Some progress has already been made through this lobbying, as noted below.
2. The potential issues for Members include that they may be at risk of loss of business or real physical danger, if the fact that they have made a SAR is revealed to a client or a third party. However, the Institute's assessment is that the risks are remote and are reducing, as the consistent lobbying on the matter referred to above has resulted in increased Government awareness of the potential political damage that could arise in this respect, and consequently has resulted in increasingly effective action. The Institute is not aware of any member having experienced a physical attack and the instances of damage to members' business interests that are reported to us have always been very few in number, though of course each of these is very worrying in its own right.
3. Some of the concerns expressed, and the expectations of members are unrealistic - SARs are submitted for the purpose of their use in the prevention, detection and prosecution of crime, including tax evasion. This cannot be done without the relay of the information contained in those SARs to the appropriate Law Enforcement Authorities (LEAs) including the tax authorities, where appropriate. In addition, the UK judicial system does not permit any guarantee to be given in respect of confidentiality, and it is not realistic to ask for such.
4. In addition, there are a number of procedures which could be put in place by firms themselves, to reduce the likelihood of inappropriate disclosure of SARs. Some of these are considered below.
5. The control of crime is in the public interest, support of which is a Charter obligation of the Institute. The new ICAEW Code of Ethics notes in its opening sections that the reliance of third parties on the objectivity and integrity of the profession imposes a public interest responsibility on the profession. A professional accountant's responsibility is not exclusively to satisfy the needs of an individual client or employer. In this environment, it follows that the Institute and profession must support the proper operation of the SARs regime, including the making of SARs by members, in a positive and cooperative manner, whenever they are required to do so.

GOVERNMENT POLICY ON THE CONFIDENTIALITY OF SARs

6. All parties concerned have a mutual interest in the proper operation of the SARs regime, including the Home Office, who have issued Guidance to Police Forces and others, on the confidentiality of SARs, for the protection of SARs reporters. This confirms that it will be a disciplinary offence for the confidentiality of SARs to be compromised, without due cause. A copy of the relevant Home Office Circular is available from their web site, at <http://www.knowledgenetwork.gov.uk/HO/circular.nsf/79755433dd36a66980256d4f004d1514/3ea52c7344053585802570d10054abc7?OpenDocument>. It has further been confirmed by the relevant Home Office official, by letter to the MLAC Reporting and Feedback Working Group, that further LEAs, including HMR&C, the Crown Prosecution Service and the Asset Recovery Agency have also agreed to apply that Guidance. The Home Office Guidance was issued after consultation with sector representatives from the regulated sector through the MLAC Reporting and Feedback Working Group. Whilst welcomed as a step forward, this guidance did not meet the request of those representatives for a statutory code in this area, and lobbying will continue.
7. Responsibility for the SARs regime has recently been taken over by the Serious Organised Crime Agency (SOCA). In July of 2005, Sir Stephen Lander, the chairman of SOCA, was asked to carry out a comprehensive review of the SARs regime (the SARs Review – copy available from http://www.soca.gov.uk/downloads/SOCAtheSARsReview_FINAL_Web.pdf) The SARs Review acknowledges (paragraph 69 and 70) the request made by the regulated sector and the undertaking to review the impact and effectiveness of the Home Office Guidance through the MLAC Reporting and Feedback Working Group. In addition, the SARs Review contains two recommendations, 13 and 14, for actions to improve the confidential handling of SARs and to provide a channel for expression of concern in particular cases.
8. SOCA have facilitated the use of SARs by LEAs, by allowing direct access by a number of them to the electronic SARs database (known as ELMER). Access to ELMER by each end user is governed by a Partnership Agreement which details the terms of reference for access, handling and confidentiality. All end users accept obligations of confidentiality in the handling of SARs as a condition of access to the database. The exploitation of SARs by end users is governed by the terms of the Home Office Circular, which is issued to end users as part of the Partnership Agreements, and signed at a senior level, to ensure commitment.
9. SOCA have also introduced a number of other systems to safeguard the confidentiality of SAR originator details. Specialist training and accreditation for LEA Financial Investigators (FIs) includes a module which deals specifically with confidentiality of SARs. Provision has been made for the quality of SARs work (including breaches of confidentiality) as well as proceeds of crime work more generally, to feature in Her Majesty's Inspectorate of Constabularies (HMIC) inspection programmes. All breaches of SAR confidentiality received by SOCA are investigated thoroughly and expeditiously with the relevant end user. SOCA are also in the course of setting up a 'Confidentiality Hotline' for the reporting sectors to raise concerns about the inappropriate use of SARs or breaches of SAR confidentiality. This is expected to be fully operational by 1st October 2006.

10. In the current environment, the Institute is aware of only four reasons why the source of a SAR might be revealed by LEAs (Including by SOCA – formerly NCIS) in a way which might result in the information getting back to a client or other suspect. These are:
 - Disclosure required by law, for the fair administration of justice
 - Disclosure by a LEA which has not signed up to the Home Office Guidance, or the SOCA confidentiality systems.
 - Disclosure by corrupt or criminal officials
 - Disclosure due to administrative error.
11. These are considered further below, together with some circumstances which have been cited as a possible reason why SARs might be disclosed, but where we believe there to be little or no justifiable cause for concern. These include:
 - Disclosure under the Freedom of Information Act; and
 - Disclosure in response to a Subject Access Request under the Data Protection Act.

DISCLOSURE REQUIRED BY LAW

12. This is covered in detail in the linked Home Office Guidance. Disclosure will very occasionally be required, for the proper administration of justice, and because of prejudice to the human rights of a defendant in a criminal case. This is so uncommon, that we are not aware of any case where it has caused harm to a member of the Institute, or been reported publicly. There are many reasons why a prosecuting authority need not include a copy of a SAR under defence disclosure, including most commonly the fact that the prosecution will not rely on the information contained therein, in making its case, nor is the information likely to weaken the prosecution's case. Further reasons for not making disclosures can include Public Interest Immunity, if a strong case can be made that the balance of the public interest lies with non-disclosure. Ultimately, the prosecution can consider withdrawing from the case, if the safety of a SAR reporter is at issue.
13. The actual harm we have seen being caused to members by the disclosure of SARs has arisen by poor practice by LEAs who had not signed up to the Home Office guidance, or administrative errors.

LAW ENFORCEMENT AUTHORITIES NOT COVERED BY HOME OFFICE GUIDANCE

14. Occasionally, a SAR is passed to a LEA which has not appreciated the importance of the confidentiality of SARs, has not yet signed up to the Home Office Guidance and has not carried out appropriate training of its investigators. An example which came to our notice in the early months of 2006 was in relation to one particular Government Agency, where an investigator revealed that a client's accountant had made a SAR, when questioning them in the course of an investigation. Strong representations were made without delay, through the Home Office and SOCA, and hopefully, this will not be repeated with that agency.

15. Needless to say, if we hear of any other LEAs, which are casual or irresponsible with SARs information, we will repeat this exercise. Relevant information should be passed to the SOCA confidentiality hotline, copied to the Institute's Head of Business Law (currently Felicity Banks) for action. Recommendation 13 in the SARs Review, which specifically suggests that all "end-users" (i.e. LEAs) "should accept obligations of confidentiality in the handling of SARS as a condition of access to the ELMER database", is clearly being implemented. A key reason for our lobbying for a statutory code of practice was to ensure obligations attached to all end-users. Whilst we will still press for a code, this implementation is a welcome step forward.
16. Less easy to control, are the actions of LEAs overseas. However, SARs will not be passed overseas, except to Financial Intelligence Units (FIUs) which are members of The Egmont Group (<http://www.egmontgroup.org/>). Members of this Group have signed up to Principles for Information Exchange Between FIUs, which includes the following:

E. Confidentiality – Protection of Privacy

13. All information exchanged by FIUs must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with national provisions on privacy and data protection. At a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving FIU.
17. If the information is then passed to overseas LEAs at all, it is sanitised so that it does not show details of the reporter.

CORRUPT OR CRIMINAL DISCLOSURE

18. This heading has been included for completeness, although the Institute has not been made aware of any occasion when a SAR has been disclosed with criminal intent by any member of the law enforcement community. If it were to occur, it would of course, be a matter of utmost concern and sensitivity to the Government and law enforcement. If members have reason to suspect that such disclosure has taken place, they should report the matter to the SOCA confidentiality hotline without delay.

DISCLOSURE DUE TO ADMINISTRATIVE ERROR

19. The most serious instances of the disclosure of SARs which have come to the attention of the Institute have all been due to administrative error. It is not possible to legislate to prevent all such instances, but this does not absolve the Government and LEAs from doing everything they can to minimise such occurrences, both by training and other procedures to prevent them happening and by strong disciplinary action against the perpetrators of any such lapses. Government consider the Home Office Guidance will improve focus on correct handling as, at least in the Police forces, the status of the Guidance means breach will be eligible for disciplinary action against the individual concerned.

20. Members are invited to inform the SOCA confidentiality hotline of any such instances, copied to the Institute's Head of Business Law, so that the Institute can ensure that they are treated seriously by the LEA involved.

DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT

21. The disclosure of information contained in individual SARs will not be necessary under the Freedom of Information Act. The Act is very wide in the scope of its requirements for disclosure of information from all public authorities, but it also has a number of strong exemptions from disclosure. These include absolute exemptions and qualified exemptions. Where an absolute exemption applies, a public authority need not confirm or deny that it holds the information, nor communicate the information if held. For qualified exemptions, the public authority must consider whether the public interest in not disclosing the information (or in not confirming or denying that they hold the information) outweighs the public interest in disclosure. The exemptions include:
- Investigations and proceedings conducted by public authorities. (Qualified)
 - Law enforcement. (Qualified)
 - Personal information. (Absolute)/(Qualified)
 - Information provided in confidence. (Absolute)
 - Statutory Prohibitions on disclosure. (Absolute)
22. Any or all of these exemptions are likely to apply, in the case of money laundering SARs. Further information on the provisions of this Act are available from the Audit & Assurance Faculty Technical release "Guidance on the Implications of the Freedom of Information Act 2000" AUDIT 02/05, available from <http://www.icaew.co.uk/index.cfm?route=115566>.

DISCLOSURE UNDER A SUBJECT ACCESS REQUEST UNDER THE DATA PROTECTION ACT

23. Disclosure of SARs to the suspect may sometimes be required under the Data Protection Act, under a Subject Access Request, but normally only by the accountancy practice, not by an LEA, and even then only:
- if the data is personal information held in a relevant filing system within the meaning of the Act;
 - if the information was obtained from an internal report, and one where the MLRO has judged that it need not be reported on to SOCA; and
 - the disclosure of the information would be unlikely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.
24. Guidance on disclosure under the Data Protection Act is available from the Treasury web site on http://www.hm-treasury.gov.uk/media/112/23/money_laundering.pdf. Though this Guidance was issued in April 2002, and refers to predecessor legislation on Anti-Money Laundering, it is still applicable, and should be interpreted in the light of the current legislation.

25. MLROs are advised to retain internal SARs, even where they judge that an external report to SOCA is not necessary, because (for example) a series of internal reports concerning a potential suspect may result in suspicion, where each individual report is considered trivial. In addition, MLROs need to retain such records to be able to respond to any enquiries from LEAs including in respect of allegations of failure to disclose pursuant to sections 330-331 of the Proceeds of Crime Act 2002. For this reason a record of internal reports is considered to be part of records that are useful for the prevention or detection of crime, and disclosure of the internal reports are accordingly very likely to be validly judged as likely to prejudice such use. In these circumstances, they would not be subject to disclosure under a Subject Access Request.

IMPLICATIONS FOR CIVIL CASES

26. As well as the current anti-money laundering provisions, the Proceeds of Crime Act 2002 introduced extensive provisions for the confiscation and recovery of criminal proceeds. SARs information may be used by LEAs not just for the purposes of criminal investigations and prosecutions, but also for intelligence leading to the civil recovery of the proceeds of crime or unlawful conduct. The same safeguards on confidentiality of SARs will apply in these cases, as for criminal cases. There are similar issues where disclosure to the party defending an action for confiscation is required, for the proper administration of justice, with similar controls over disclosure, in the interests of reporters. Civil recovery of criminal proceeds is an important and growing tool being used in the fight against crime – in particular in the case of organised crime, where the controlling minds may be far removed from the people actually carrying out each criminal act. The public interest in making SARs reports will apply equally to SARs used from civil recovery as for criminal action, but equally, the confidentiality of the SARs reporter needs to be guarded.

SELF HELP

27. The likelihood of the inadvertent disclosure of a SAR can be reduced by the introduction of appropriate reporting procedures by the accountancy practice making the report. Such procedures might include:
- mentioning the name of the firm and the MLRO only in the “front sheet” of a standard SAR reporting form, not elsewhere, such as in the “reasons for suspicion” box. This will help enable LEAs to pass information to investigation teams which does not include the identity of the reporter, and reduce the likelihood of inadvertent disclosure.
 - Where it is clear that the information is likely to be key evidence in a prosecution, firms can request the LEA to serve them with a production order covering the background information which led the SAR to be made in the first place. This should help make it clear to the client that information was passed to law enforcement under compulsion within the terms of a Court order.
 - Where there is particular reason to fear that a suspect might be motivated to try and discover whether a SAR had been made and by whom, and take revenge (for example where a SAR might involve a suspect with a known history of violence, or

where organised crime or a terrorist organisation might be involved) this should be brought to the attention of Law Enforcement. This might be done by the inclusion of a note (in bold type, at the top) in the SARs reporting box on reason for suspicion.

- Proper house-keeping of the MLRO's records should be maintained, to ensure that Personal Data (as defined under the Data Protection Act) is only retained where it continues to have information value likely to be useful for the prevention or detection of crime, and hence where its disclosure would be likely to be prejudicial in that context.

28. In the past, the Institute has become aware of a number of instances where inappropriate disclosure of SARs arose because of problems due to the acknowledgement of hard copy SARs going astray, or being opened in the post rooms of member firms. This might have occurred because of a number of reasons, including:

- firms failing to use their full names and details to identify themselves as the reporter, resulting in a number of cases of acknowledgements being sent to firms with identical or similar names; and
- post rooms obeying standing instructions to open all incoming mail, even where marked "confidential" and "addressee only".

29. NCIS also had a number of administrative problems of its own, partly caused by a shortage of resources to deal with the many thousands of SARs they were sent. In addition, they were the subject of much criticism for failing to acknowledge SARs on a timely basis, or at all. SOCA has decided that the way they will deal with this family of problems is not to acknowledge hard copy SARs at all, and set up an automatic system for the acknowledgement of SARs submitted on their new system for the electronic submission of SARs. The Institute supports this change of policy on the acknowledgement of SARs, as being the lesser of two evils.

CONCLUSION

30. As can be seen by the content of this Note, the confidentiality of SARs continues to be a key area of attention, in the Institute's representational work on money laundering matters. It is an area where we have lead the regulated sector lobbying efforts through our continuing off the public record work in the MLAC Reporting and Feedback Working Group. We have achieved some real improvements to date, and have created the opportunities to press for further improvements. A high level of trust and credibility has been built between our representatives and the leadership of SOCA (the new owner of the SARs regime) that we will continue to use, with the aim of strengthening the SARs reporting regime, in the public interest and that of our members.

31. Continued reporting of particular instances of inappropriate disclosure of SARs should be reported to the SOCA confidentiality hotline, copied to the Institute's Head of Business Law (currently Felicity Banks) as they occur, with as much background information as possible, so that they can be addressed on a case-by-case basis and used as background material in our continued lobbying.

FJB