FINANCIAL INTELLIGENCE UNIT (UKFIU) BULLETIN

Suspicious Activity Reports (SARs) - Top Ten Tips for the Accountancy Sector

This is a United Kingdom Financial Intelligence Unit (UKFIU) communications product, produced in line with the Serious Organised Crime Agency's (SOCA) commitment to share perspectives on the Suspicious Activity Reports (SARs) regime.

SOCA
SERIOUS ORGANISED CRIME AGENCY

SOCA is a Home Office Non-Departmental Governmental Body

April 2011

Suspicious Activity Reports (SARs) - Top Ten Tips for the Accountancy Sector

Accountancy Sector Vetted Group Project

In 2009 the Vetted Group[1]undertook a thematic review of SARs submitted by the accountancy sector[2]. The aim of the project was to produce material to assist the accountancy sector in providing good quality SARs by identifying examples of good and bad practice, identify gaps in quality and business segment reporting.

In order to facilitate this project SOCA provided the Vetted Group with access to a dataset of over 1,500 accountancy SARs submitted over a three month period. This included both standard and Consent SARs. The majority of the SARs were submitted by small and medium sized businesses.

The thematic review proved to be a successful exercise providing useful analysis of SARs submitted by the accountancy sector. This has allowed SOCA to draw on the results of the review to develop the following sector specific Top Ten Tips. It is hoped that this document will assist and encourage accountancy reporters to submit more good quality SARs and promote consistency across the sector.

This approach has been endorsed by the supervisors[3] who regulate those that operate within accountancy sector as defined under the Money Laundering Regulations 2007. We acknowledge their ongoing support of the SARs regime.

[1] The Vetted Group is a group of security cleared stakeholders from across the SARs regime, which meets to provide a forum for gaining expert input on intelligence developments in a confidential environment.
[2] The definition of 'accountancy sector' incorporates all those individuals and entities acting as auditors, insolvency practitioners, external accountants, tax advisers or providers of accounting services as defined under the Money Laundering Regulations 2007.
[3] A list of supervisors can be found on page 9.

1) Use SAR Online to submit

SAR Online is a secure web based system by which you can quickly and easily submit SARs to SOCA. Surprisingly, 20% of all SARs within the sample had not been submitted online. Over 90% of the non-electronic submissions were from smaller businesses.

Registering with SAR Online is a very simple process and ensures that SAR submissions are delivered directly to SOCA. This is particularly pertinent in the case of Consent issues. Reporters that submit SARs via SAR Online will also receive an acknowledgement email containing a unique reference once the report has been submitted.

At SOCA we appreciate that changing working practices can be daunting, and to make this less of a concern all new reporters who register on SAR Online receive a welcome pack containing guidance on submitting SARs, an overview of the SARs Regime, case studies and useful contacts. Reporters also receive case-by-case quality reviews of their SARs one month and six months after registration.

For further details of this service please refer to the links at the end of this document.

2) Initial summary

It is good practice to open the SAR with a brief summary to illustrate the reasons for suspicion and provide a chronological sequence of events detailing the dates of any activity or transactions. Keep all SAR content clear, concise and simple.

3) Provide explicit details of the reason for 'suspicion'

In 21% of the SARs submitted within this sample there was insufficient information provided to indicate how their reason for suspicion had originated. To illustrate this, actual ‘reasons for suspicion’ taken from the study sample are shown below:

- ‘No sales receipts’
- ‘Lack of supporting evidence’
- ‘Accounts filed at Companies House’

The content and quality of a SAR can affect the UKFIU’s ability to prioritise and process the report and Law Enforcement Agencies' (LEAs) decision or ability to investigate. Often a seemingly irrelevant piece of information can become a valuable piece of intelligence.

Therefore when you provide information giving the reasons for your suspicion, ask yourself this question: if I knew nothing about this matter, would I be able to understand what had been the trigger for suspicion? To assist you, try to answer the following six basic questions to make the SAR as useful as possible: Who? What? Where? When? Why? How? Remember to include the date of activity, the type of product or service, how the activity will or has taken place and the reason for suspicion.

4) Include all known details relating to the subject of the SAR

It is accepted that in some cases the amount of personal detail relating to the individuals who were reported against may be limited - for example, where the subject of a SAR is the client’s employee. However, in circumstances where the subject of the SAR is the client, a large amount of information should already be held for the purpose of Customer Due Diligence.

Please provide all relevant Customer Due Diligence detail known about the person reported. This should include, as a minimum, full name/s, date of birth, nationality and address.

If further information is held about the person - for example identification document details (including relevant reference or document numbers), additional addresses (ensuring that the status is clearly indicated i.e. current, previous, home, business, other known property ensuring that postcodes are included), car details, telephone numbers (clearly marked home, business, mobile etc.), full details of bank accounts or other financial details (including account numbers etc.) then these can be of great importance and should be included on the SAR wherever practicable.

5) Include the context of your reason for submitting the SAR

Include details of the background that led to the submission of a SAR - for example, the nature of the business activity you were engaged in with the person or business against which you submitted the SAR. In over 50% of the sampled SARs there was no indication of the type of service being provided: for example - audit, insolvency, taxation etc. It may be interesting to note that the omission of this detail was uniformly apparent across the whole sample - irrespective of the size of the business submitting the report.

6) SARs must not be used as a communication channel

The study sample illustrated that some members of the accountancy sector were using the submission of a SAR as a means of obtaining advice. For example, some Consent SARs were clearly submitted as a means to gain advice as to whether a particular form of action on their behalf would constitute a 'Tipping Off' offence.

Please remember that SARs are only for the reporting of suspicious activity to SOCA. If you need to seek general guidance relating to money laundering or the SARs Regime in particular, you can contact your regulatory body, your designated Money Laundering Reporting Officer (MLRO) or SOCA.

7) Avoid the use of acronyms or jargon within SARs

The sample of SARs reviewed for the Vetted Group survey identified that 15% of the disclosures contained either acronyms or the use of jargon. The use of acronyms and jargon should be discouraged as they may not be understood by the recipient and may be open to misinterpretation.

If you are describing a service provided or a technical aspect of your work it would be beneficial to provide a brief synopsis to aid the financial investigator who may not have accountancy experience.

8) Reporting of an acquisitive crime or fraud related crime

When you have knowledge or suspicion of an acquisitive or fraud related crime, you will be faced with a parallel decision making process. Firstly, you will have to decide

whether or not you wish the offence to be investigated and to report the crime. You can report an acquisitive crime to your local police force.

In cases of confirmed fraud, private individuals and small and medium sized businesses can make a report through Action Fraud via www.actionfraud.org.uk or telephone 0300 123 2040. In addition, the National Fraud Desk at the National Fraud Intelligence Bureau takes reports of serious fraud from corporate bodies. The National Fraud Desk can be contacted by email at nfd@cityoflondon.pnn.police.uk or by telephone 020 7601 6999.

Secondly, regardless of whether or not a crime report has been made, you will have to consider your legal obligations under the Proceeds of Crime Act 2002. If you have knowledge or suspicion that a money laundering offence has taken place and criminal property has been derived then you must submit a SAR to SOCA (unless the privilege reporting exemption applies). Where the matter has been reported as a crime you are encouraged to include the Crime Reference Number in the top line of the 'Reason for Suspicion' field of the SAR.

9) Obtaining Consent

Obtaining Consent provides a defence against specific money laundering offences. A Consent SAR must be submitted if, during the course of your normal business activity, you are asked to carry out an activity or transaction that you know or suspect would constitute a prohibited act under s327-329 of the POCA 2002 and under Part 3 of the Terrorism Act (TACT) 2000 as amended by the TACT 2006.

What if I decline to facilitate the requested suspicious activity or transaction?
By gaining the consent of SOCA to carry out the suspicious transaction you may provide time for LEAs to carry out an investigation to ascertain if the activity or transaction is lawful or not. This will enable them to take whatever enforcement or intervention action that may be appropriate.

How long does this take?
SOCA will notify you within seven working days as to whether Consent has been granted. If notification is not received, then Consent may be assumed on the eighth working day. If you need to submit a Consent SAR, ensure that you tick the ‘Consent’

box on the form and provide a detailed account of the particular activity for which you believe Consent is required.

What if Consent is refused?
Where SOCA refuses Consent, the transaction or activity must not proceed for a further 31 calendar days or, if earlier, until further notified by SOCA.

10) Use of the SAR Glossary of Terms

The SAR Glossary of Terms is used to identify specific categories of suspicious activity. This allows members of the SARs Regime, particularly law enforcement, to identify SARs in which they have a specific interest. The inclusion of the appropriate Glossary Term can be very useful in ensuring the distribution of the SAR to the correct law enforcement or government agencies.

Need advice or assistance with a SAR?

If you require any further help or advice please visit www.soca.gov.uk. Alternatively, for information or assistance with submitting SARs, SAR Online enquiries and Consent issues, the UKFIU can be contacted as follows:

Tel: 020 7238 8282
Press '2' – SAR Admin enquiries
Press '3' – SAR Online enquiries
Press '4' – Consent

General UKFIU matters may be emailed to the Dialogue Team at ukfiusars@soca.x.gsi.gov.uk.

For advice locally, please speak to your designated MLRO and refer to the Money Laundering guidance published by your regulatory body.

Useful partner links

Association of Accounting Technicians (AAT) – www.aat.org.uk

Association of Chartered Certified Accountants (ACCA) – www.accaglobal.com

Association of International Accountants (AIA) – www.aiaworldwide.com/MoneyLaundering

The Association of Taxation Technicians (ATT) – www.att.org.uk

Chartered Accountants Regulatory Board (CARB) – www.carb.ie

Chartered Institute of Management Accountants (CIMA) – www.cimaglobal.com/Members/Members-handbook/Anti-money-laundering/Suspicious-activity-reporting-to-soca

The Chartered Institute of Taxation (CIOT) – www.tax.org.uk

The Chartered Institute of Public Finance and Accountancy (CIPFA) – www.cipfa.org.uk

HM Revenue and Customs – www.hmrc.gov.uk

The Institute of Chartered Accountants in England and Wales (ICAEW) – www.icaew.com

The Institute of Financial Accountants (IFA) – www.ifa.org.uk

Insolvency Practitioners Association (IPA) – www.ipa.uk.com

National Fraud Intelligence Bureau (NFIB) – www.nfib.police.uk

Serious Organised Crime Agency (SOCA) – www.soca.gov.uk/threats/money-laundering

The Institute of Chartered Accountants of Scotland (ICAS) – www.icas.org.uk/site/cms/contentcategoryview.asp?category=4424

The Institute of Certified Bookkeepers (IOCB) – www.bookkeepers.org.uk

Disclaimer

While every effort is made to ensure the accuracy of any information or other material contained in or associated with this document, it is provided on the basis that SOCA and its staff, either individually or collectively, accept no responsibility for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any such information or material.

Any use by you or by any third party of information or other material contained in or associated with this document signifies agreement by you or them to these conditions.


aat


ACCA


A·I·A
THE ASSOCIATION
OF INTERNATIONAL
ACCOUNTANTS


att
The Association of Taxation Technicians


carb
Chartered Accountants
Regulatory Board


CIMA
Chartered Institute of
Management Accountants


CIOT
Chartered
Institute of
Taxation
Excellence in Taxation


CIPFA
The Chartered Institute of
Public Finance & Accountancy


HM Revenue
& Customs


ICAEW


ifa
Est. 1916
Institute of Financial Accountants


50
Insolvency
Practitioners
Association
1961 - 2011


National Fraud
Intelligence Bureau


SOCA
SERIOUS ORGANISED CRIME AGENCY


QUAERE VERUM
THE INSTITUTE OF
CHARTERED ACCOUNTANTS
OF SCOTLAND


MAKING YOU COUNT
THE INSTITUTE
OF CERTIFIED
BOOKKEEPERS

Protecting this document

This is a government document that has been graded as NOT PROTECTIVELY MARKED. There are no specific requirements for storage or disposal and it can be considered as safe for wide distribution within your organisation. This can extend to its use for training or awareness programmes for staff. However, unless otherwise specified, this information is not intended for general public dissemination and should not be included on public facing websites, external mailing lists, social media or other outlets routinely used by you to deliver information to the public. We therefore request that you risk manage any onward dissemination in a considered way.

UKFIU Dialogue Team

The aim of the Dialogue Team is to drive the UK Financial Intelligence Unit (UKFIU) agenda on interfacing with stakeholders on Suspicious Activity Reports (SARs) activity. The team strives to improve communication and understanding between the SARs Regime's participants, to increase the value extracted from the SARs Regime, to provide, facilitate and contribute to various fora and to share perspectives on the operation of the Regime as a whole. In essence the Dialogue Team seeks to improve the quality of SARs intelligence, and promote the value and greater use of this intelligence in mainstream law enforcement activity.

For further information, please contact the SOCA UKFIU Dialogue Team by email ukfiusars@soca.x.gsi.gov.uk or by telephoning 0207 238 8282. For more information about the Serious Organised Crime Agency go to www.soca.gov.uk.

Reducing harm – Providing information back to SOCA

We would like to remind you of the provisions contained in Section 34 Serious Organised Crime and Police Act 2005. These provisions say that any information provided by you to SOCA, in order to assist SOCA to discharge its functions which include the prevention and detection of crime, will not breach any obligation of confidence which you may owe to any third party or any other restriction on the disclosure of information. S34 requires that disclosures of personal information about living individuals by you to SOCA must still comply with the provisions of the Data Protection Act 1998 (DPA), but you may be satisfied that disclosure by you of such personal information to SOCA in order to assist SOCA to prevent and detect crime is permitted by the DPA. Please, therefore, submit all S34 information to ukfiusars@soca.x.gsi.gov.uk.

Handling advice – Legal information

This information is supplied by SOCA under Section 33 of the Serious Organised Crime and Police Act 2005. It is exempt from disclosure under the Freedom of Information Act 2000. It may also be subject to exemption under other UK legislation. Except where permitted by any accompanying handling instructions, this information must not be further disclosed without reference to SOCA in accordance with Section 35(1) of the Serious Organised Crime and Police Act 2005.

This report may contain 'Sensitive Material' as defined in the Attorney General's guidelines for the disclosure of 'Unused Material' to the defence. Any sensitive material contained in this report may be subject to the concept of Public Interest Immunity. No part of this report should be disclosed to the defence without prior consultation with the originator.

Requests for further disclosure which are not permitted by any handling instructions or handling code must be referred to the SOCA originator from whom you received this information, save that requests for disclosure to third parties under the provisions of the Data Protection Act 1998 or the Freedom of Information Act 2000 and equivalent legislation must be referred to SOCA's Public Information Compliance Unit by e-mail on picuenquiries@soca.x.gsi.gov.uk.