FINANCIAL INTELLIGENCE UNIT (UKFIU)

Submitting a Suspicious Activity Report (SAR) within the Regulated 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 sharing perspectives on the Suspicious Activity Reports (SARs) Regime.

SOCA
SERIOUS ORGANISED CRIME AGENCY

SOCA is a Home Office Non-Departmental Governmental Body

November 2012

Submitting a Suspicious Activity Report (SAR) within the Regulated Sector

Overview

This document seeks to provide advice and relay best practice when making a Suspicious Activity Report (SAR), a piece of information that alerts Law Enforcement Agencies (LEAs) that certain client/customer activity is in some way suspicious and might indicate money laundering or terrorist financing.

Persons in the regulated sector are required under Part 7 of the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 (TACT) to submit a SAR in respect of information that comes to them in the course of their business, if they know, or suspect or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, money laundering or terrorist financing. A SAR must be submitted as soon as is practicable.

This document seeks to complement the Money Laundering Regulations and HM Treasury approved guidance in this regard. It is important that when submitting a SAR to SOCA that reporters refer to the published guidance from their own regulatory body and their own internal guidance.

By submitting a SAR to the Serious Organised Crime Agency (SOCA) you will be providing LEAs with valuable information of potential criminality whilst ensuring appropriate compliance with your legal obligations to report under POCA and TACT.

You are able to submit SARs in any format including by post, fax or via the SOCA website (www.soca.gov.uk) through the SAR Online system.

Once you have submitted your SAR, you should remember your obligation not to make a disclosure to anyone, which is likely to prejudice any investigation that might be conducted following the making of the SAR. You must also not disclose that any investigation into allegations that an offence under Part 7 of POCA has been committed, is being contemplated or is underway. If you do so, you may commit a "tipping off" offence as defined by section 333 of the Proceeds of Crime Act 2002 or section 21D of the Terrorism Act 2000.

SOCA does not provide or approve standard wording for you to use in such circumstances. It is therefore recommended that you give careful consideration to how you will handle your relationship with the subject once you have submitted the SAR, particularly if the subject is a client or customer of your business.

SAR Online

SAR Online is a secure web based system by which you can quickly and easily submit SARs to SOCA. Registering with SAR Online is a very simple process and ensures SARs are delivered directly to SOCA, including an activation process to create the account for the submission of SARs. SAR Online is SOCA's preferred means of SARs submission and provides a standardised approach to structuring SARs that reporters may find useful. It is important to provide as much comprehensive detail as possible when registering.

Use of SAR Online is recommended as:

- It will provide you with an automated acknowledgement of receipt.
- It will help you structure your SAR in the most helpful way, thereby improving processing time in SOCA.
- It will give you the opportunity to flag the SAR as a consent issue.

Reporters that submit SARs via SAR Online will also receive an acknowledgement email containing a unique reference once the report has been submitted. The submission of consent SARs is particularly valuable to ensure a prompt response.

In order to register for SAR Online, new users require an active email account as this is used as your user identification. The registration is unique to the user so the email address needs to be designated to the appropriate person. It is recommended that the Money Laundering Reporting Officer (MLRO), Nominated Officer or designated officer responsible for the Anti-Money Laundering (AML) compliance within the organisation is the registered user.

SOCA understands that the process can seem daunting when you first begin. There is a dedicated support team available during office hours to deal with any SAR Online enquiries. The SAR Online Helpdesk can be contacted on 020 7238 8282, option 3.

Further support is available on the SOCA website www.soca.gov.uk or through your professional body or regulator.

However if you are not reporting electronically please use the SOCA Preferred Forms for manual reporting which can be downloaded from the SOCA website.

Reason for suspicion

Making a quality report, structured in a logical format and including all relevant information, will significantly enhance LEAs' abilities to extract greater value from submitted SARs. Often a seemingly minor piece of information to you can become a valuable piece of intelligence to LEAs.

The SAR Glossary of Terms (available on the SOCA website www.soca.gov.uk) is used to identify specific categories of suspicious activity and is widely used by law enforcement enabling them to identify SARs in which they have a specific interest. The inclusion of the appropriate Glossary Term can be useful in ensuring the distribution of the SAR to a law enforcement or government agency which may be best placed to utilise or act on the information provided. However, use of the SAR Glossary of Terms is not mandatory.

It is helpful to write a brief summary to illustrate succinctly your suspicions when submitting a SAR and provide a chronological sequence of events, i.e. describing the events, activities or transactions that led you to be suspicious, how and why you became suspicious, and where appropriate, the nature of the business activity you were engaged in, details of dates of any activities or transactions etc. Try to keep the content clear, concise and simple.

If the reported subject (i.e. client/customer) has been the subject of a previous SAR submitted by your organisation, it is valuable to include the previous SAR reference number if appropriate to do so and glossary code XXS2XX. However, please also remember that under POCA and TACT, each SAR you submit on the same individual must contain a suspicion and all the relevant details; even if you have included the reference number for a previously submitted SAR.

As a basic guide, wherever you can, 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, and how the activity will take place or has taken place, when documenting the reason for suspicion.

If you are suspicious because the activity deviates from the normal activity for that customer/business sector, it would be helpful to briefly explain how the activity that gave rise to your suspicion differs.

Avoid the use of acronyms or jargon within SARs 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 in your SAR to aid the financial investigator. We recommend you do not send attachments with your SAR – all the relevant information should be within the SAR. If further information is available which you are willing to share with an LEA then reference to this and who to contact may be recorded in the SAR.

Subject information

The amount of information a reporter holds on the reported subject may be dependent on the Customer Due Diligence (CDD) obtained in line with guidance published by its firm and supervisory body. It is helpful to those who will use your SAR to be as comprehensive as possible; however, you are only required to provide information obtained within the ordinary course of your business.

Please note: If you are submitting a SAR using SAR Online you are requested to fill in the subject information within the fixed fields provided for the purpose.

Individuals

Please provide all relevant details known about the individual reported. The amount of information you will have may well depend on the relationship to the reported subject. Please provide all identifying information. This should include, as far as possible, drawing on CDD records: full name/s, date of birth, nationality and address.

It is important that the status of the address/es can be fully understood i.e. current, previous, home, business, and other known property, ensuring that postcodes are included.

If further information is held about the individual – for example:

- identification document details (including relevant reference or document numbers) e.g. passport, driving licence, National Insurance number.
- car details (registration number)
- telephone numbers (clearly marked home, business, mobile etc)
- full details of bank accounts or other financial details (including account numbers etc)
- occupation

then the information can be provided in context with your suspicion.

Businesses, trusts and other entities, incorporated and unincorporated

1) Incorporated

Please provide all relevant details known about the incorporated entity. This should include:

- full name
- designation e.g. Limited, SA, GmbH
- trading name
- registered number
- VAT and/or tax reference number
- country of incorporation
- business/trading address
- registered office address.

Additionally, please provide details of the individuals or entities that are the directors (or equivalent) and details of the individuals who own or control or exercise control over the management of the entity.

2) Unincorporated

Please provide all relevant details known about the unincorporated entity. This should include:

- full name
- business/trading address
- VAT and/or tax reference number.

Additionally, please provide details of all partners/principals who own or control or exercise control over the management of the entity.

3) Trusts

Please provide all relevant CDD details known about the trust. This should include:

- full name of the trust
- address
- nature and type of the trust.

Additionally, please provide details of all trustees, settlors, protectors and known beneficiaries as appropriate.

Description of criminal property and its whereabouts

When the suspicion being reported relates to a financial transaction, the report should include the relevant details of the beneficiary/remitter of the funds and, if known, the destination/originating bank details e.g. sort code, correspondent bank details. It is important to accurately record the date on which the transaction has occurred or will occur. It is also useful to understand the type of transaction - for example online payment/receipt, debit or credit card, ATM withdrawal, cheque, electronic transfer (BACS/CHAPS), or cash.

If the beneficiary/remitter of the transaction is believed to be complicit in the suspicious activity then consideration should be given to providing their details as an associate subject. An associated subject is a person or entity that is linked to the main person/entity in some direct way and is involved in the suspicious activity.

If the activity does not involve a financial transaction then an explanation of the suspicious activity that has occurred or will occur should be given.

When submitting a SAR using SAR Online there are fields for documenting specific financial transactions. Equally, transactions or activity can be documented within the 'reason for suspicion' field provided.

Appropriate consent

Obtaining consent provides a defence against the principal money laundering offences. Should you wish to avail yourself of this you should refer to a separate document which has also been published on the SOCA website (www.soca.gov.uk) entitled *'Obtaining consent from SOCA'*. This provides specific guidance on the process to be followed and what to expect if you wish to apply to SOCA for a consent decision.

If you are using SAR Online you are reminded to ensure you tick the appropriate Consent Box when completing your SAR. In all cases it is important to specify clearly the activity for which consent is required.

Threshold Requests

Section 339A of POCA makes provision for a threshold in the case of deposit-taking institutions in operating an account if it is £250 or less without the need to seek consent. If the proposed activity exceeds £250, permission to vary the 'threshold' payment is required from SOCA before the activity may be conducted. The reporter should still make a disclosure in respect of the initial opening of an account or, if different, the time when the deposit-taking body first suspects that the property is criminal property.

If you are submitting a SAR with a Threshold Request, please specify the threshold amount sought, the account it relates to, and details of the frequency and nature of the activity to which the threshold will relate, including the value. If a threshold is already in place and you wish to seek a variation, then the reasons for the variation will need to be clearly defined.

Please note:
A threshold request is not the same thing as a consent request and there are no statutory timescales for dealing with them. However to facilitate threshold requests, SOCA uses the consent desk to progress the responses and it is helpful if the consent box is ticked on the SAR to enable the desk to identify the requests quickly.

Court orders and law enforcement enquiries

In some instances, you may be served with or have notice of a court order such as a production order, made in respect of a particular individual or entity. This may act as a catalyst for you to review the activity which you conduct or have conducted in relation to that individual or entity.

If, following such a review, you feel that there is an obligation to submit a SAR or seek consent, then the SAR/consent request should reflect your suspicions in the context of your engagement with the subject.

Acquisitive 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.

SOCA does not take crime reports from the public in the same way that a police force would. If you believe a crime has been committed, the matter should be reported to the relevant 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 and can be contacted by telephone 020 7601 6999.

Secondly, regardless of whether or not a crime report has been made, you will wish to consider your legal obligations under the Proceeds of Crime Act 2002 (POCA). If you have knowledge or suspicion that a money laundering offence has taken place then you must submit a SAR to SOCA.

SOCA's advice from its police partners is that where a reporter wishes the content of a SAR to be formally recorded as a crime report they should report this directly to their local police force. Where the reporter has reported a crime and, in addition, has submitted a SAR, it would be helpful if the crime reference number could be included in the top line of the text in the SAR so that it can immediately be cross-referenced by law enforcement.

Alerts and keywords

The Alerts process is a recognised and established way by which SOCA communicates with the UK's private sector. These are written communications that warn of a specific risk, threat or problem. All Alerts contain a keyword or a glossary code. If you submit a SAR on the strength of an Alert please include the keyword within the free text field.

SAR confidentiality

The confidentiality of SARs is the cornerstone of the reporting regime. SARs are held on a secure central database within SOCA and access to the database by law enforcement is strictly controlled by SOCA.

The use of SARs is governed by Home Office Circular No. 53/2005 (*Money Laundering: The Confidentiality And Sensitivity of Suspicious Activity Reports [SARs] And The Identity Of Those Who Make Them*). All law enforcement agencies using SARs are required to follow the guidance outlined

If reporters have concerns about the inappropriate use of SARs by Law Enforcement Agencies (LEAs), or breaches of SAR confidentiality, they should call the SAR Confidentiality Breach Line on freephone 0800 234 6657 (9am-5pm, UK time, Monday to Friday). This number is for reporting breaches of confidentiality only.

Contacting SOCA UK Financial Intelligence Unit (UKFIU)

SARs should not be used as a communication channel e.g. as a means of gaining advice. 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 are advised to contact your designated Money Laundering Reporting Officer (MLRO) or your regulatory body.

For information or assistance with submitting SARs, SAR Online enquiries and consent, please visit www.soca.gov.uk or contact the UKFIU as follows:

Tel: 020 7238 8282
Press '2' - General SAR enquiries
Press '3' - SAR Online helpdesk
Press '4' - Consent SAR enquiries

When contacting the UKFIU please have available your SAR reference number if applicable.

General UKFIU matters may be emailed to ukfiusars@soca.x.gsi.gov.uk

If you wish to make a SAR by post you should address your SAR to UKFIU, PO Box 8000, London, SE11 5EN or by fax on 0207 283 8286. You are reminded that post and fax are slower than SAR Online and therefore it will take longer for your SAR to be processed. You will not receive an acknowledgement if you use post or fax.

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.

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 safe for wide distribution within your organisation and for use in staff training or awareness programmes.

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 participants, to increase the value extracted from the SARs regime, to provide, facilitate and contribute to various forums 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 SOCA Dialogue Team by email at finrelteam@soca.x.gsi.gov.uk. 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 of the 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