

FINANCIAL INTELLIGENCE UNIT BULLETIN

Independent Financial Advisors (IFAs), Mortgage Brokers and Retail Intermediaries: Identifying Risks to Your Business and Reporting Suspicious Activity

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



SOCA is a Home Office Non-Departmental Governmental Body

August 2010

Purpose of bulletin

This is a United Kingdom Financial Intelligence Unit (UKFIU) document that supports the key SOCA objective of sharing information and intelligence based around the Suspicious Activity Reports (SARs) Regime.

This product can be used to raise awareness, increase knowledge, develop understanding, support training and underpin joint working programs.



The impact of crime and the financial advisory sector

The Home Office estimates that serious organised crime in the UK generates approximately £20 billion a year. As the anti-money laundering (AML) regime continues to tighten, money launderers and those involved in serious and organised crime are using increasingly sophisticated methods to launder their proceeds of crime rather than placing funds directly into the more traditional vehicles such as banks. These methods include the use of financial professionals which give launderers access to a wide range of products and services; the financial advisory sector is both attractive and vulnerable to criminal groups laundering and disguising funds.

Within this sector mortgage brokers, for example, are particularly at risk as the purchase of property both in the UK and overseas continues to be a common method used by serious organised criminals to launder the proceeds of their criminal activity. The advantage of doing so is that large amounts of criminal funds can be 'cleaned' in a single transaction.

This document is intended to help the financial advisory sector to:

- Understand some of those issues
- Identify some of the techniques used by criminals
- Provide practical guidance on reporting suspicious activity to SOCA under the regulations.

This Bulletin is marked **NOT PROTECTIVELY MARKED**.
Please comply with the handling instructions at the end of this document.

Why serious organised criminals seek the acquisition of financial products

Although it may be a sector belief that there is little risk of becoming involved in money laundering from criminals, the risk posed to financial advisors from serious organised criminals in the UK is considerable.

Whether that risk comes from being exploited in order to launder drug money, arranging a mortgage for a residence to be used for human trafficking, or simply as a method of appearing to be a legitimate business representative, the financial advisory sector can be undermined by a lack of knowledge of how criminal groups and individuals operate.

It is believed that a significant proportion of serious organised criminals purchase financial products via an independent financial advisor (IFA) in an attempt to further distance themselves from financial institutions and thereby conceal the proceeds of their crime.

Vulnerability of the financial advisory sector

Firms that do not implement adequate procedures to safeguard against the risks leave themselves open to exploitation by serious organised criminals. These criminals routinely seek out useful people they can exploit along with new opportunities to advance their growing criminal interests. If necessary, they use criminal methods (e.g. bribery, coercion) to elicit co-operation.

Firms with inadequate procedures are also vulnerable to prosecution by the Financial Services Authority (FSA) for non-compliance with AML regulations.

How the sector is misused and abused

Two product types are particularly vulnerable to abuse: mortgages and investments. The use of property is a well-known method for criminals to launder their funds and they frequently use mortgages despite their having cash to buy property outright.

Again, laundering through investments is a well known typology, with a common method being the investment of a lump sum in a policy to then surrender it after a short period and obtain a cheque from the product provider in the hope of making funds appear legitimate.

It is also likely that some IFAs are unwittingly used by criminals to launder the proceeds of crime and gain access to insurance and investment products to improve their lifestyle. This will include criminals who buy products in the same way as law-abiding citizens but using the proceeds of crime to pay for them.

Take steps to safeguard yourself, your business and your employees

Identifying the risks

Useful information can be found on the financial crime section of the FSA website:
www.fsa.gov.uk/Pages/About/What/financial_crime/index.shtml

Specific threats to businesses and investment products are listed in the Joint Money Laundering Steering Group (JMLSG) Guidance Notes Part II 'Sectoral Guidance'.

Knowing your responsibilities

As part of the regulated sector IFAs, mortgage brokers and retail intermediaries are required to conduct their business in accordance with the necessary defined standards (Money Laundering Regulations 2007).

The FSA provides clear working guidance on these standards, and industry guidance, such as the JMLSG Guidance Notes, give more detail on the regulatory requirements.

The Regulations carry criminal as well as regulatory sanctions.

Knowing your business

By understanding normal business patterns, you can identify the unusual or unexpected:

- A client investing more than their net worth would suggest is possible
- The early surrender of investment products, especially if incurring a loss
- A client receiving monies from offshore accounts, especially if there is no reason for this
- A client requesting products that are inappropriate to their financial situation
- A client receiving or sending monies via a (unidentified) Third Party
- A client switching products on a frequent basis
- A client changing investment patterns
- Any attempt to purchase financial products in cash
- A client appearing to be living beyond their means
- A client with business activity or funds inconsistent with the industry average

Knowing your customer

By exercising due diligence in taking steps to inspect and verify client identity documents, you may identify anomalies. Examples include:

- Use of false documentation
- Reluctance to provide personal details
- Doubts about the source of client funds
- Refusal to provide the requisite proof of identification or residence
- Inconsistencies in documentation such as anomalies in dates, photographs or signatures

Knowing your limits

By taking into account this information, you can determine how risk aware your business should be, given the range and nature of its activities.

As you conduct business, consider the risks and ask yourself: is this a risk I am willing to take?

(The previous examples should not be construed as a checklist of suspicious activity. They are for illustrative purposes only and are by no means exhaustive).

Tax evasion

Tax evasion is a criminal offence irrespective of the amount involved and whether Her Majesty's Revenue & Customs (HMRC) is prepared to settle on a civil basis. Suspected tax evasion, including deliberate under-declaration of income or the intentional over-claiming of expenses, falls within the definition of money laundering.

It is reportable to SOCA even if HMRC are already aware of it. Investing funds on which tax has been evaded may result in an advisor committing a s328 'arrangements' offence under the Proceeds of Crime Act 2002 (POCA).

Reporting suspicious activity to law enforcement

A Suspicious Activity Report (SAR) is a piece of information that alerts Law Enforcement that a certain client/customer activity is in some way suspicious and may indicate money laundering or terrorist financing.

A SAR should be submitted as soon as you '**know**' or '**suspect**' a person is engaged in money laundering or dealing in criminal property. Submitting a SAR provides a defence against committing a money laundering offence: it protects you, your business and your reputation. Failure to submit a required report is a criminal offence.

The SOCA electronic SAR Online system will allow your business to submit SARs in a secure and efficient manner and to receive a prompt acknowledgement.

The SAR Online system is accessible through a link on the SOCA website (www.soca.gov.uk). These reports are held on a secure database and held in the strictest confidence.

Further help or guidance is available on the website. SOCA has a dedicated support team that provides a helpdesk facility to address any obstacles encountered with SAR Online. The support team is available 9am to 5pm Monday to Friday (excluding Bank Holidays). Please telephone 020 7238 8282 and select option '3' from the menu.

Useful links

Serious Organised Crime Agency (SOCA) www.soca.gov.uk
Joint Money Laundering Steering Group (JMLSG) www.jmlsg.org.uk
Financial Services Authority (FSA) www.fsa.gov.uk
Financial Action Task Force (FATF) www.fatf-gafi.org
Association of Independent Financial Advisors (AIFA) www.aifa.net
Association of Mortgage Intermediaries (AMI) www.a-m-i.org.uk
Association of Professional Compliance Consultants www.apcc.org.uk

Comments and feedback

In order to assist SOCA UKFIU in improving this service, we welcome any feedback you may have on this particular product and the information provided. Please email the UKFIU Dialogue Team inbox at ukfiusars@socax.gsi.gov.uk, quoting the code "FF333FF".

UKFIU CONTACTS

UKFIU 020 7238 8282

Press '2' - SAR Management
Press '3' - SAR Online
Press '4' - Consent

Confidentiality Hotline
0800 234 6657

Postal Address
UKFIU
PO Box 8000
London
SE11 5EN

Email
ukfiusars@socax.gsi.gov.uk

DISCLAIMER

While every effort is made to ensure the accuracy of any information or other material contained in 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 information or other material contained herein.

Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.

© 2010 Serious Organised Crime Agency



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.

UKFIU Dialogue and Special Projects Team

The aim of the Dialogue and Special Projects 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 UKFIU Dialogue and Special Projects Team by email at ukfiusars@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.