

MONEY LAUNDERING LAW

A REGULATORY NEWS UPDATE FROM DLA PIPER



UK NEWS

HMRC's strategic framework for tackling **CRIMINAL FINANCES**

Taking the profit out of crime stands as a central tenet of the Government's agenda, involving the Treasury, the Home Office, the Assets Recovery Agency ("ARA"), the Serious Organised Crime Agency ("SOCA") and Her Majesty's Revenue and Customs ("HMRC").

On 24 May 2007, HMRC published its high-level strategic framework which seeks both to provide overarching objectives for each of the government agencies involved in tackling criminal finances and to maximise the use of the new powers provided by the Serious Organised Crime and Police Act 2005.

The objectives of this framework are to:

1. maximise seizures of cash and other negotiable instruments which result in forfeiture by:

- establishing a National Financial Intelligence Branch;
- making quality interceptions at the borders and inland by having a workforce equipped with appropriate skills and equipment;
- focusing on innovation and the sharing of best practice and management information;

2. maximise the value of criminal proceeds recovered through confiscation by:

- ensuring that financial investigation with a view to confiscation is a feature of all criminal investigations;
- seeking restraint orders at the earliest appropriate stage in an investigation;

3. use tax laws to tax criminal profits and civil proceedings to recover criminal assets by:

- referring cases to the ARA for civil actions;
- recycling funds from the Asset Recovery Incentivisation Scheme into new measures to attack criminal activity; and

4. identify opportunities to undermine criminal financial gains further by pursuing money-laundering offences in addition (or as an alternative) to other offences by:

- maximising intelligence flows through the financial intelligence officers located within SOCA;
- taking action against money-laundering offences, especially in cases of serious fraud and for those in positions of responsibility; and
- further developing close relationships with key players in order to drive investigation efforts against targeted money launderers.

The Assets Recovery Agency publishes annual report and launches consultation

On the same day that HMRC published its strategic framework document, the ARA issued its annual report.



This showed that in 2006 it:

- recovered £15.9m worth of criminal wealth;
- obtained recovery orders, voluntary settlements and issued tax assessments to a value of £16.6m; and
- disrupted assets worth £73.6m in a further 114 cases.

This represents five times the amount of crime-related assets seized five years ago, before the current more aggressive policies were in place. The government has also announced it hopes to double again the amount seized by 2010.

To further this aim, the police are looking for a number of changes

which extend their powers of seizure. These include:

- new powers to seize 'status-setting' acquisitions, such as diamond jewellery and plasma screen TVs, from those charged with burglary and robbery;
- seizing both cash and assets, like boats and cars, which have been used in crimes or are the proceeds of crimes;
- incorporating recovery of the proceeds of crime into criminal sentencing;
- offering citizens a percentage of the goods or money seized for whistleblowing on fraud committed against the government; and
- removing the time limit for seizing crime-related assets.

The public is encouraged to comment on the proposals contained within the Asset Recovery Action Plan by 23 November 2007 (details of the consultation are available on the Home Office website).

Protecting Charities from terrorism - joint consultation launched

May also saw the launch of a joint consultation initiated by the Home Office and the Treasury: *Review of Safeguards to Protect the Charitable Sector from Terrorist Abuse*. The risk of charitable activities being seen as a soft option for terrorist finance or for providing a veil of legitimacy to the financing of terrorist networks has been recognised by the Financial Action Task Force ("FATF")¹, whose

Special Recommendation VIII requires that all countries review the adequacy of their relevant laws and regulations.

In February 2006, the Treasury and the Home Office began an assessment of existing safeguards for the charitable sector. Their conclusion is that, while the current scale of terrorist links is extremely small in comparison to the size of the sector, the scope for exploitation could become

significant without immediate, appropriate and co-ordinated action by government, the regulator (the Charity Commission) and the charities themselves. By publishing the review (available on the Home Office website), the Government is seeking to consult all stakeholders in order to establish the best policy framework going forward. The consultation period ends on 2 August 2007.

¹ The Financial Action Task Force is an inter-governmental body set up in 1989 for the development and promotion of national and international policies to combat money laundering and terrorist financing

SOCA'S APPROACH UNDER SCRUTINY IN COURT OF APPEAL

In a recent Court of Appeal case², the Law Lords rebuked SOCA for its “unlawful action” in freezing payments to a company the agency believed may have been involved in a VAT fraud. They also granted permission for the appellant company, UMBS Online, to apply for judicial review.

In summary, the facts of the UMBS case are as follows:

- UMBS is an offshore finance company, operating solely over the internet, which provides instant money transfers. The key to its business is that it can transfer money around the world very quickly.
- UMBS used Currency Solutions Limited (“CS”) to process external bank transfers. CS had, in turn, arranged for Laiki Bank to set up trust accounts for UMBS' customers' monies.
- UMBS began to experience delays with payment requests and discovered that CS had made a disclosure to SOCA concerning its suspicions about UMBS. SOCA had replied to CS granting consent to the release of UMBS's funds under section 335 of the Proceeds of Crime Act 2002 (“POCA”).
- Subsequently, Laiki Bank also had suspicions and made a disclosure to SOCA. This time, however, consent was refused and UMBS transactions were frozen.
- Solicitors for UMBS asked SOCA to reconsider its refusal. SOCA responded on 27 February 2007 stating: “Refusal of consent is effective until the expiry of the moratorium period of 31 days..... In the absence of a further request for consent from Laiki Bank and a change in circumstances, the refusal of consent will not be revisited by the Serious Organised Crime Agency.”
- UMBS applied to the court for a judicial review but, at the first hearing, was not successful. The court concluded that SOCA had no obligation to look at requests from third parties (ie UMBS) and SOCA's change of heart (by refusing consent to Laiki Bank) was rational as there was an ongoing investigation.

COURT OF APPEAL

UMBS appealed and the Court of Appeal reversed the earlier judgment. In particular, the court held:

- The response from SOCA on 27 February 2007 was not rational and SOCA was asked to reconsider.
- The change of heart was not rational because there had, at that stage, been no investigation. UMBS also argued that the procedure applied by SOCA did not comply with Article 1 of the First Protocol of the European Human Rights Convention³. The court noted that SOCA did not have prescribed procedures for dealing with consent requests. As Lord Justice Sedley's comments seem to suggest, the Law Lords are concerned about SOCA's powers: “In setting up the Serious Organised Crime Agency, the state has set out to create an Alsatia - a region of executive action free of judicial oversight.”

Following the Court of Appeal decision, SOCA reconsidered its refusal of consent, again refused and, in addition, obtained a restraint order. The Court of Appeal has, however, directed that the judicial review continue.

² *UMBS Online Limited (“UMBS”) v SOCA and HMRC* [2007] EWCA Civ 406

³ Article 1, Protocol 1 states: “every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.”

FRAUD ADVISORY PANEL CALLS FOR LEGISLATION TO BE EXTENDED INTO “VIRTUAL WORLD”

The growth of “virtual world” gaming websites has, in recent years, significantly increased. A combination of chat rooms and 3D games, these virtual communities allow users to create fantasy worlds where they choose what they look like and what they do. They have now become so popular that many of these websites have spun-off marketplaces where intangible goods and services are bought and sold with real money and where pretend currency, used within the virtual world, is exchanged for hard currency. It is estimated that on an average day about £750,000 changes hands.

Unsurprisingly, such websites have become the latest target for online crime and the Fraud Advisory Panel, the independent watchdog, is calling for the government to ensure that all existing laws and regulations cover this evolving area and that virtual funds exchanged in this way count as genuine financial instruments. The panel has identified a number of problems arising with virtual communities:

- tax evasion and unregulated cross-border money movements;
 - credit card fraud against genuine customers and suppliers;
 - sales of age-restricted goods and services to minors.
- hacking into databases and identity theft;
 - new opportunities for money laundering via false online identities;
 - the possibility of being used by organised gangs attempting to avoid surveillance;

Of further concern is the need to determine exactly which jurisdiction's laws apply, given the borderless nature of the virtual worlds and the prevalent culture of anonymity where it is often difficult to know with whom any one player is dealing.

Anti-money laundering guidance from Law Society on legal professional privilege

Subsequent to the 2005 decision in *Bowman v Fels*⁴, solicitors were advised that common law legal professional privilege still applied to the commission of the principal money laundering offences. In these circumstances, if consent was not given by the client to waive that privilege so that a report could be made to SOCA, the solicitor had to withdraw from acting for that client.

More recently, the Law Society's Money Laundering Task Force has received advice from senior counsel on a number of aspects of the *Bowman v Fels* decision.

The Task Force has declared itself satisfied that the existence of common law legal professional privilege will amount to a “reasonable excuse” for not reporting under sections 327 (2)(b), 328(2)(b) and 329(2)(b) of POCA. This means that a solicitor will not be deemed to have committed a principal offence by continuing with the transaction, despite not making a report to SOCA. The decision of whether to continue with their client's instructions under these circumstances will remain a question of ethics.

⁴ *Bowman v Fels* [2005] EWCA Civ 226 [2005] 1 W.L.R. 3083 [2005] 4 All E.R. 609 [2005] 2 Cr.App.R. 19 [2005] 2 C.M.L.R. 23 [2005] 2 F.L.R. 247 [2005] W.T.L.R. 481 [2005] Fam. Law 546 (2005) 102(18) L.S.G. 24 (2005) 155 N.L.J. 413 (2005) 149 S.J.L.B. 357 [2005]

Government accedes on clearer money laundering **REGULATIONS**

Ministers have bowed to pressure from the Law Society and other professional bodies to revise the draft regulations implementing the Third European Directive on Money Laundering (the "Directive"). As the Law Society's president had pointed out to the Treasury, "It is unacceptable for the Government to pass the responsibility of interpreting the incomprehensible language of this Directive to solicitors, who face possible imprisonment if they get it wrong." Of particular concern was the definition of "beneficial ownership" used in the Directive, which counsel, instructed by the Law Society, held to be unlawful

within an English context. In addition, it was feared that the regulations would impose significant additional costs on solicitors for compliance and reduce the competitiveness of UK law firms as a result.

The current draft regulations provide for customer due diligence procedures to be extended into the area of trusts. Lawyers providing services to trusts would be required to undertake checks to establish the identity of beneficiaries who own at least 25% of a trust and then to verify the identity of those persons. It was predicted that the additional expense thereby

incurred would be passed on to clients. The Treasury has now said that it will publish a full version of the revised rules by the end of June, having already communicated its planned changes to the FSA, the Office of Fair Trading, the British Bankers' Association, the Law Society and the Institute of Chartered Accountants in England and Wales.



Ministers have bowed to pressure from the Law Society and other professional bodies to revise the draft Regulations implementing the Third European Directive on Money Laundering (the "Directive").

“POLITICALLY EXPOSED PERSONS”- IMPLICATIONS FOR THE FINANCIAL SERVICES INDUSTRY UNDER THE NEW REGULATIONS

Politically Exposed Persons (PEPs) are individuals whose prominent position in public life gives them opportunities to profit from corruption. As a result, the money-laundering risk associated with PEP customers is greater than for many other types of clients. The good practice guidance promoted by FATF and the Joint Money Laundering Steering Group (“JMLSG”) since 2003 will finally be codified when the new Money Laundering Regulations (“Regulations”) come into force this December and, for the first time, the Regulations will provide a legal definition of PEPs in the UK. They will also require firms to have risk-based procedures in place to identify foreign PEPs and to apply enhanced customer due diligence (“CDD”) measures to these customers on a risk-sensitive basis.

DEFINING PEPs

The draft Regulations define a PEP as “an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions”. The definition extends to the post-holder’s immediate family members and known close associates and includes a non-exclusive list of PEP categories. The onus will be on firms to decide whether or not to add other categories, in line with the general risk-based approach of the Regulations. Domestic holders of prominent positions and junior and middle-ranking officials are, for instance, excluded from the definition but, where firms believe the money-laundering risk relating to such individuals is high, they will be required to apply enhanced CDD measures under the general obligation. It might, also, be appropriate in certain situations to continue to apply the measures to former PEPs for longer than the period of one year after they have left public office.

IDENTIFYING PEPs

It is envisaged that identifying a PEP will come from a firm’s usual customer due diligence and “know your customer” procedures. Such procedures are meant to be appropriate to the level of risk associated with any given customer, product or service. It is not intended, however, that every customer be treated as a potential PEP. Where normal procedures do, however, reveal the need for more detailed investigation into a customer’s background, a number of resources will be available. The FSA advises that these may range from asking additional questions and undertaking a simple internet search to subscriptions to commercially available databases deemed more appropriate to firms with a high level of PEP exposure.

ASSESSING THE RISK

Having identified a PEP, firms are given the latitude by the Regulations to determine the extent to which they apply enhanced CDD measures. In doing so, however, firms are required, on a risk-sensitive basis, to:

- obtain appropriate senior management approval for establishing a business relationship with a PEP customer;
- take adequate measures to establish the source of funds which are involved in the business relationship or occasional transaction; and
- conduct enhanced ongoing monitoring of the business relationship.

The application of these measures is not optional as it will become a legal requirement.

In its recent Financial Crime Newsletter⁵, the FSA has stressed that the obligation to identify PEPs on a risk-sensitive basis does not amount to an obligation to identify every PEP a firm comes across but only to identify those who pose a real money-laundering risk and to take measures to mitigate this risk effectively. As such, and for many, the new Regulations will simply require the translation of current good practice (promulgated in the JMLSG Guidance 2006) into a legal obligation rather than the imposition of entirely new obligations.

FSA fines BNP Paribas Private Bank for weak ANTI-FRAUD CONTROLS

The FSA has fined BNP Paribas Private Bank ("Bank") £350,000 for weaknesses in its systems and controls which allowed an employee to transfer £1.4m fraudulently out of clients' accounts without permission. The 13 fraudulent transactions were carried out between February 2002 and March 2005 using forged clients' signatures and instructions and by falsifying change of address documents.

Following an investigation, the FSA found that the Bank did not have an effective review process for large transactions (over £10,000) from clients' accounts. The Bank was also found wanting in its procedures (which were not clear) regarding the role of senior management in checking significant transfers prior to payment. Together, this had resulted in a number of fraudulent transactions not being independently checked. Additionally, a flaw in the Bank's IT systems had allowed the senior employee to evade the normal middle office processes so that basic authorisation and signatory checks were not carried out on internal cash transfers between different customer accounts.

This is the first time a private bank has been fined for weaknesses in its anti-fraud systems. As Margaret Cole, the FSA's Director of Enforcement, said, "This is a warning to other firms that we are raising our game in this area and expect them to follow suit."



EU AND INTERNATIONAL NEWS

EUROPEAN ANTI-FRAUD OFFICE MAKES ITALIAN ARRESTS OVER CITRUS FRUIT FRAUD

The Italian law enforcement authorities in Calabria, in co-operation with the European Anti-Fraud Office ("OLAF"), announced in April of this year that 45 suspects had been arrested in the course of an investigation into alleged fraud against EU aid paid for the withdrawal and processing of fresh citrus fruit from the market. Pursuant to Council

Regulation n° 2202/96, European Community aid is available for those producers of lemons, grapefruit, oranges, mandarins or clementines who deliver fruit grown in the EU for processing into juice. In the course of the investigation it emerged that most, if not all, of the fruit supposedly consigned to the processors by the producer organisations in

question was fictitious. Hence, the investigation concluded that the concentrated juice supposedly sold by the firms and upon which European Community aid was claimed and paid, was equally non-existent. The potential damage to the EU budget is estimated to be up to €50m.

European Commission official under suspicion of corruption

Following a complaint received by OLAF, an investigation in Belgium has brought to light suspicions of corruption, the manipulation of tender procedures and fraud in the context of the leasing and procurement of EC delegation buildings and their security installations in countries outside the EU. The main persons under suspicion at this stage are a European Commission official, an assistant of a

Member of the European Parliament and the manager of a private company.

At the end of March 2007, the Brussels Prosecution Service announced that three arrests were made, the main offences alleged being: corruption of a civil servant; violation of professional secrecy; and criminal conspiracy.

EVALUATION OF TURKEY MADE BY FATF

Turkey is the eleventh country to be assessed on the implementation of anti-money laundering and counter-terrorist financing standards in the FATF's third series of mutual evaluations of its members.

Key findings were:

- the number of convictions for money laundering is relatively low and the related legislation has not been in place for sufficiently long to be able to demonstrate its effectiveness;
- confiscation measures have, also, not yet produced substantial results;
- the number of suspicious transaction reports received by the relevant Turkish authority is low;
- that customer due diligence measures need to be significantly reinforced in order to meet fully FATF standards;
- Turkey also needs to put comprehensive anti-money laundering/counter-financing of terrorism obligations into place for designated non-financial businesses and professions in order to comply with the FATF standards.

Transparency International reports on ANTI-CORRUPTION MEASURES IN AFRICA

Nine African countries (Algeria, Burundi, Kenya, Liberia, Nigeria, Sierra Leone, South Africa, Togo and Uganda) were assessed by Transparency International ("TI")⁶ to have failed to implement fully international anti-corruption conventions. TI undertook a series of country-focused studies which

analysed anti-corruption measures and highlighted the main shortcomings of the reform process. The society also noted that by April 2007 only 16 of 53 African countries had ratified the African Union Convention on Preventing and Combating Corruption.



DEFICIENCIES IN ANTI-BRIBERY LAWS IDENTIFIED IN UK AND JAPAN

The Ministerial Council Meeting of the Organisation for Economic Co-operation and Development ("OECD") met on 15 May 2007 amid calls from TI to make enforcement of its Anti-Bribery Convention a central focus of the meeting. TI urged the OECD to call on all signatory governments to correct deficiencies in their laws promptly and to undertake enforcement at a level sufficient to bring about the required change in corporate conduct in international transactions. The UK and Japan were singled out for particular criticism. The chair of TI, Huguette Labelle, expressed the view that:

"It is of particular concern that the group of non-enforcing countries includes the UK and Japan, two of the world's largest exporters. Continuing this lack of enforcement undermines the collective commitment by the major industrialised states to stop competing and undermining local governance efforts on the basis of bribery."

In contrast to a number of cases brought in France, Germany, Italy, Norway, Spain, Sweden and the United States against major multinational firms, TI also expressed disappointment at the UK government's decision in December 2006 to terminate an

investigation into allegations of bribery on a Saudi project by BAE Systems. They also pointed to the UK's planned postponement until 2009 in addressing what is seen as antiquated laws on corruption.

⁶ Transparency International is a politically non-partisan, global society dedicated to fighting corruption.

Regulated by the Law Society.

DLA Piper UK LLP and **DLA Piper Scotland LLP** are part of DLA Piper, a global legal services organisation, the members of which are separate and distinct legal entities. For further information please refer to www.dlapiper.com/structure

A list of offices can be found at www.dlapiper.com

UK switchboard +44 (0) 8700 111 111



INVESTOR IN PEOPLE

For further information please contact:

Daren Allen, Partner, London Office

T: 020 7796 6824

E: daren.allen@dlapiper.com

F: 020 7153 7710

This publication is a general overview and discussion of the subjects dealt with and is up to date as at the end of May 2007. It should not be used as a substitute for taking legal advice in any specific situation. DLA Piper UK LLP and DLA Piper Scotland LLP accept no responsibility for any actions taken or not taken in reliance on it.

Where references or links (which may not be active links) are made to external publications or websites, the views expressed are those of the authors of those publications or websites which are not necessarily those of DLA Piper UK LLP or DLA Piper Scotland LLP and DLA Piper UK LLP and DLA Piper Scotland LLP accept no responsibility for the contents or accuracy of those publications or websites.

If you would like further advice, please contact Daren Allen.

This material was originally published by LexisNexis UK in June 2007.