LLOYD'S

MARKET BULLETIN

REF: Y4161

Title	Money Laundering
Purpose	To update Market Participants on developments in Money Laundering legislation
Type	Updated Money Laundering Guidance
From	Andy Wragg, International Market Access 020 7327 6387 or andy.wragg@lloyds.com Rachael Connor, International Market Access 020 7327 6380 or rachael.connor@lloyds.com
Date	13 June 2008

MONEY LAUNDERING GUIDANCE

PURPOSE

On 15 December 2007, new anti-money laundering ("AML") regulations became effective in the UK, namely the Money Laundering Regulations 2007 ("the Regulations"). These follow implementation of the EU's Third Money Laundering Directive, the Directive on the prevention of Money Laundering and Terrorist Financing (2005/60/EC). The purpose of this bulletin is to update Compliance Officers and Money Laundering Reporting Officers ("MLROs") in the Lloyd's market on the new regulations in conjunction with the existing legal and regulatory framework, clarify its impact on the Lloyd's market and advise on best practice guidance. Consultation has been held with the FSA, Serious Organised Crime Agency ("SOCA") and the Market in putting together this guidance.

The expanded guidance at Appendix 1 covers:

- Overview of impact on General Insurance and Managing Agents
- The stages of Money Laundering
- The Legal and Regulatory Framework
- Application to Members' agents
- General Practical Guidance
- Statistics of suspicious reports made to Lloyd's

A listing of useful external sources of information appears at Appendix 2.

SUMMARY OF KEY GUIDANCE POINTS

Scope of Legislation

- General insurance and most managing agents fall outside the regulated sector for Proceeds of Crime Act ("PoCA") and the Regulations but fall within those offences under PoCA which apply to all persons and the non regulated sector as well as offences under the Terrorism Act ("TACT") 2000 which apply to all persons.

- Members' agents and life syndicates fall under the regulated sector of PoCA and the 2007 Regulations as well as TACT 2000.

PoCA and TACT offences

- The PoCA offences and their application to each sector or to all persons are:

o **Concealing etc (s.327)* - All Persons**
o **Arrangements (s.328)* - All Persons**
o **Acquisition, use and possession (s.329)* - All Persons**
o **Disclosure requirements (s.330) - Regulated sector/any staff, (s.331) - Regulated Sector/nominated officer, (s.332) - Non-regulated Sector/other nominated officers)**
o **Tipping off:**
  - **Disclosing a Suspicious Activity Report ("SAR")/investigation (s.333A (1) and s.333A (3)) - Regulated sector**
  - **Prejudicing an investigation (s.342 2 (a))- Non-regulated sector, and (s.342 2 (b)) - All Persons**

Primary Offences

- A SAR made to SOCA under PoCA which may include consent to proceed with a transaction is a defence to a disclosure offence.

- A disclosure to Lloyd's MLRO, Sean McGovern, from the Market for the purposes of reporting to SOCA, will not constitute a Tipping off offence.

- Certain disclosures to parties other than SOCA are permitted including disclosure to a person's supervisory authority and will not trigger the Tipping Off offences.

- Consent from SOCA is required to proceed with a transaction which is suspected to involve suspicious activity. This can be requested from SOCA via Lloyd's MLRO or by the managing agent/members agent itself.

- If 7 working days have expired without a response from SOCA or if consent has been refused by SOCA but a further 31-day period has expired without any notification whether law enforcement has acted to restrain the transaction, then the transaction can go ahead.

- All MLROs will commit an offence if they consent to an employee to carry out a transaction falling under a primary offence without obtaining consent from SOCA first.

- If SOCA deems consent is not required, the already submitted disclosure can be treated as a standard SAR. Managing/members' agents should record SOCA's decision and the reason given.

- The maximum penalty for the primary offences is 14 years' imprisonment or a fine or both on conviction on indictment; and on summary conviction, a maximum imprisonment of 6 months or a fine or both.

- The disclosure and tipping off offences carry a maximum penalty of 5 years imprisonment on conviction on indictment and again on summary conviction, a maximum of 6 months imprisonment. Failure to disclose may facilitate the money laundering transaction and in so doing trigger a primary offence and a maximum penalty of 14 years imprisonment.

- TACT 2000 has one money laundering offence applicable to all persons:

    - **Facilitation or retention or control of terrorist property by concealment, removal from jurisdiction, by transfer (S18**)

- TACT disclosure requirements are under S19 for the non regulated sector to report to their MLRO where information comes to light in the course of business and under S21A for the regulated sector.

- The money laundering offence under TACT (section 18) carries a maximum penalty of 14 years imprisonment, whilst the disclosure offences on conviction carry a maximum penalty of 5 years imprisonment.

Risk Based Approach and Customer Due Diligence

- The Regulations apply to the regulated sector i.e. members' agents and life syndicates. General insurers and most managing agents have no legal obligation to comply with the Regulations, however Lloyd's recommends that its measures are implemented on a risk based, best practice approach.

- The Regulations require that a risk based approach ("RBA") towards customer due diligence is adopted by assessing whether a customer requires enhanced, simplified or no due diligence, due to its risk profile. A firm must be able to demonstrate to its supervisory authority (e.g. FSA) that the extent of CDD measures is appropriate in view of its financial crime risks.

- CDD should be carried out when "establishing a business relationship" or "carrying out an occasional transaction" to verify the adequacy or veracity of previously obtained information or where there is a suspicion of money laundering or terrorist financing but a risk assessment of the type of customer, business relationship, product, transaction or jurisdiction will determine the extent of CDD checks required.

- However, the CDD requirements not only require verifying the identity of the customer (using reliable and independent documentation) but also where applicable to identify and verify the identity of the beneficial owner and to obtain information on the purpose and intended nature of the business relationship.

- If CDD measures cannot be complied with, a regulated sector firm should cease the transaction/relationship and consider making a SOCA referral.

- Simplified CDD is appropriate where customers/transactions/products fall within certain categories considered lower risk and enhanced CDD is applicable where higher risk is perceived such as where a customer has not been physically identified and transactions involving politically exposed persons ("PEPS").

- Ongoing monitoring should be carried out to ensure customers' profiles are consistent and information up to date.

- The Regulations allow reliance on third parties for carrying out CDD (these third parties are defined in the Regulations) as long as the third party consents to their evidence being used. The firm requesting CDD is still responsible for any failure to apply CDD despite such reliance.

Compliance requirements and reporting procedures

- FSA SYSC rules 3.2 6A – 3.2.6J relate to financial crime but do not apply to general insurance. However, the general provision under 3.2.6 applies to all firms including general insurers and requires firms to have effective systems and controls, such as training, management reporting, risk management policies and money laundering risk management policies to prevent financial crime. Life syndicates/members' agents are caught by all of the above however Lloyd's expects managing agents to follow all of the SYSC principles.

- The Joint Money Laundering Steering Group ("JMLSG") Guidance 2007 advises regulated firms how to comply with legal and regulatory anti-money laundering ("AML")/counter terrorist financing ("CTF") obligations. It is formally approved by HMT and the FSA will take into account whether a firm has followed it. It is also useful for non regulated firms to follow to encourage and demonstrate best practice.

- Managing agents should have procedures in place for staff to report to their MLRO suspicious transactions that are declined (protected disclosures) or transactions requiring consent (authorised disclosures) for onwards reporting to SOCA via Lloyd's MLRO if applicable.

- Decisions and reasons not to make disclosures should be recorded by the MLRO.

- Declination of a fraudulent claim does not require reporting under PoCA although it can be reported to the Police as a fraud. If however a claim is suspected of being fraudulent but there is no evidence to decline it, we have been advised that managing agents should request consent from SOCA to pay it.

- Managing agents can report directly to SOCA but there are advantages e.g. trend analysis if reports are made to Lloyd's MLRO for onward transmission to SOCA. (Again, a disclosure to Lloyd's for the purposes of reporting to SOCA, will not constitute a tipping off offence.)

- Underwriting agents' disclosure requirements should be satisfied by making a report to Lloyd's MLRO, Sean McGovern, who has delegated the function to the International Regulatory Risk team. This can be achieved by reporting directly to Andy Wragg (see below) and to mlro@lloyds.com

- There are a number of factors which might give rise to a suspicion for business conducted in the Lloyd's Market. For a list of examples, see the extended guidance in Appendix 1.

- AML procedures should be documented and include recognising and reporting suspicious transactions, training and record keeping. They should be reviewed and enhanced if required.

- AML procedures should assess the risk profile of each business area i.e. products/channels/countries/reputational risk.

- Staff training should be provided at least every 2 years and should be properly documented and recorded.

- Records should be retained for at least 5 years.

Ongoing Activity

An appropriate RBA may be difficult to assess as there is little practical guidance for general insurers as to the measures that can be implemented as well as risk profiles varying between managing agents. Lloyd's recognises that managing agents would benefit from more assistance on this subject. Later this year, the International Regulatory Risk and Operational Risk teams will be conducting a review of all managing agents' AML/CTF/financial crime procedures so that an analysis can be drawn up and shared with the Market, which will include practical examples of factors to consider for a RBA.

This bulletin has been sent to all managing agents, approved run-off companies and members' agents and is provided to Lloyd's accredited brokers for information.

If you have any questions on this bulletin please contact Andy Wragg on 020 7327 6387 or at andy.wragg@lloyds.com or Rachael Connor on 020 7327 6380 or at rachael.connor@lloyds.com

APPENDIX 1

EXPANDED MONEY LAUNDERING GUIDANCE

1. IMPACT ON GENERAL INSURANCE AND MANAGING AGENTS

The Home Office estimates that organised crime generates over £20 billion of social and economic harm to the UK every year. All serious acquisitive crime (obtaining criminal property) is most likely to involve money laundering and can result from a number of things such as drug trafficking, handling stolen goods, trading counterfeit goods, false claims and corruption, to name a few, as well as from the traditional method of money laundering, i.e. trying to turn funds from criminal activity into clean money.

It is considered that the money laundering risk facing general insurance is lower in comparison to other financial sectors. For this reason, the insurance industry falls outside the money laundering regulated sector where general insurance is concerned.

Managing agents conducting general insurance are however subject to an element of the risk of money laundering. They are caught under those sections of Proceeds of Crime Act ("PoCA") and the Terrorism Act 2000 ("TACT") which apply to all Lloyd's market participants such as the primary offences of concealing, arranging and acquisition/use/possession and to the related "failure to disclose" and "prejudicing an investigation" offences that are applicable to the "non-regulated" sector. (See 4.1 and 4.3.) Therefore managing agents should be implementing procedures to comply with existent anti-money laundering legislation**.** Guidance on implementing procedures as well as reporting and recognising suspicious transactions are discussed at sections 6, 9 and 10 of this bulletin.

2. MEMBERS' AGENTS AND LIFE SYNDICATES

The Money Laundering Regulations 2007 ("the Regulations"), in following the scope of the 2003 Regulations, apply to members' agents and life syndicates.

In particular, the Regulations set out obligations to have systems and controls in place to identify procedures for new customers and to prevent and detect money laundering. Members' agents and life syndicates must obtain sufficient information in respect of a member/new member/applicant for life assurance in order to comply with the Regulations.

Detailed guidance on the steps firms should take to establish appropriate identification procedures to mitigate the money laundering risks posed by their customers is contained in the Joint Money Laundering Steering Group ("JMLSG") guidance notes for the financial sector. More detail on the purpose of the JMLSG and the guidance is set out at section 4.5 of this bulletin but in brief, members' agents and life syndicates will find useful Part 1, Chapter 5 of the JMLSG guidance, which explains how a firm can meet its legal obligations in the area of customer due diligence, including information to identify the customer and

understand the customer's circumstances such as source of funds/wealth. Part 2 of the JMLSG guidance consists of industry specific advice which will also assist members' agents and the life market with AML compliance.

The Regulations make it a criminal offence if the requirements to establish adequate and appropriate policies and procedures to prevent money laundering are not met by those to whom it applies, (regardless of whether or not money laundering actually takes place) and a relevant person (as defined in the Regulations) can, if found guilty, be liable to a fine and/or a prison sentence of up to two years.

3. STAGES OF MONEY LAUNDERING

The money laundering process can be broken down into 3 stages.

Placement - This is the physical disposal of criminal proceeds. In most cases, the proceeds normally take the form of cash which the criminal will attempt to place in the financial system.

Layering - This is the separation of criminal proceeds from their source by the creation of layers of transactions designed to disguise the source of funds and provide the appearance of legitimacy. This is the most likely stage at which insurers would become involved in the money laundering process.

Integration - Providing the layering process has been successful, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets.

4. THE LEGAL AND REGULATORY FRAMEWORK

The UK legislation which impacts upon the prevention of money laundering and terrorist financing currently consists of:

- The Money Laundering Regulations 2007
- PoCA 2002 (as amended)
- The Terrorism Act 2000
- FSA Handbook Provisions including SYSC 3.2.6 (see 4.4 for further information)

Guidance also exists, including:

- Joint Money Laundering Steering Group ("JMLSG") guidance (updated November 2007)

4.1 PROCEEDS OF CRIME ACT (2002) AS AMENDED ("POCA")

PoCA is a single set of money laundering offences applicable throughout the UK to the proceeds of all crimes. The offences have a broader definition than the commonly understood definition of money laundering (i.e. the movement, layering and concealment of criminal funds) and can relate to activity concerning criminal property. Whilst general insurance is low risk for the concealment and conversion of the proceeds of crime, it is, for example, at risk of fraudulent claims which, if successful, would generate criminal funds. (See section 7 of this bulletin for more details about claims fraud.)

4.1.1 Offences

There are three primary offences under PoCA, detailed below, which apply to both the regulated and non-regulated sectors i.e. to **ALL** Lloyd's market participants. They are:

Concealing etc (s.327) - Where someone knows or suspects that the property is the benefit of criminal conduct, or it represents such a benefit then he/she commits an offence if he/she conceals, disguises, converts, transfers or removes that criminal property from England and Wales, Scotland or Northern Ireland.

Arrangements (s.328) - An offence is committed by a person if he/she enters into or becomes concerned in an arrangement which he/she knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

Acquisition, use and possession (s.329) - An offence is committed if someone knows or suspects that property is the benefit of criminal conduct and acquires, uses or has possession of the property.

4.1.2 Disclosure Obligations

PoCA imposes disclosure obligations with regard to the above offences. The disclosure requirements are different according to whether a firm falls within the "regulated sector" or the "non-regulated sector". [1]

The non regulated sector applies to general insurance and long term insurance business other than qualifying contracts of insurance (as defined in Part 1 of the FSMA (RAO) 2001). For the most part, business conducted by Lloyd's managing agents falls outside the regulated sector. However syndicates writing life business and certain other types of long term insurance business (including permanent health insurance) and members' agents fall within the regulated sector.
The summary of the "failure to disclose" offence for the non-regulated sector is set out below. The "failure to disclose" offences for the regulated sector impose more onerous requirements.

S.332 - Non-regulated Sector - failure to disclose - nominated officers

[1] Schedule 9, Part 1 of PoCA defines a business in the regulated sector.

For a firm operating outside the regulated sector, a person nominated to receive disclosures under PoCA (often the MLRO) commits an offence if he/she:

1. knows or suspects that another person is engaged in money laundering; and
2. knows the identity of the money launderer or the whereabouts of the laundered money and he/she believes that the disclosure identifies the money launderer or will assist in identifying the money launderer or the whereabouts of the laundered money; and
3. does not make the required disclosure as soon as practicable after the information comes to him/her.

Thus, MLROs/nominated officers in the non-regulated sector must assess suspicious activity reports made to them and if conditions 1 to 2 are satisfied they must make the appropriate disclosure.

Technically, the offence of non-disclosure in the non regulated sector is applicable to nominated officers only and not to other staff. However it should be noted that if staff were to fail to report a transaction they were suspicious of they could still find themselves facing a primary offence. For example, if the transaction went ahead and resulted in a crime being committed, the staff member may be deemed to have assisted the criminal to launder the proceeds of his/her activities (see 4.1.6 Penalties below).

The disclosure requirement is satisfied by making a report to the Serious Organised Crime Agency (“SOCA”). (See Section 6, Reporting Suspicious Transactions.)

S330 - Regulated Sector - failure to disclose - any staff
A person commits an offence if:

1. he/she knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering; and
2. that the information or other matter on which his/her knowledge/suspicion is based or which gives reasonable grounds for such knowledge or suspicion came to him/her in the course of business in the regulated sector; and
3. he/she does not make the disclosure as soon as practicable after the information/matter comes to him/her.

The disclosure must be made to a nominated officer or to a person authorised i.e. SOCA for the purposes under PoCA.

S331 - Regulated Sector - failure to disclose - nominated officers
A person nominated to receive disclosures commits an offence if:

1. he knows or suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering; and

2. that the information on which his knowledge or suspicion is based or which gives reasonable grounds for such knowledge or suspicion came to him as a consequence of a disclosure under section 330 above; and
3. If he does not make the required disclosure as soon as practicable after the information or other matters come to him.

The person does not commit an offence if he/she has a reasonable excuse (not defined) for not disclosing the information or other matter.

It is a defence to the three offences above that disclosure of the potential offence has been made to SOCA and consent to proceed has been sought (if appropriate) or that there are reasonable grounds for non disclosure.

4.1.3 Tipping off

The tipping off offences are contained in the Proceeds of Crime Act 2002 as amended by the Proceeds of Crime Act 2002 (Amendment) Regulations 2007 (POCA regulations 2007).

There are also tipping off offences for terrorist property in TACT, as amended by the TACT Regulations 2007.

S333A - Tipping off - regulated sector – all staff

There are two tipping off offences under this section, both of which apply to the regulated sector:

S333A (1) - Disclosing a suspicious activity report ("SAR") – regulated sector – all staff

It is an offence to disclose to a third party that a SAR has been made by any person to SOCA, a nominated officer, the police or an officer of Revenue and Customs if such disclosure is likely to prejudice any investigation that might be conducted as a result of the SAR. This offence can only be committed after a SAR has been made, if it is known or suspected that such disclosure is likely to prejudice any investigation related to that SAR and the information upon which the disclosure is based came to light in the course of business in the regulated sector.

S333A (3) - Disclosing an investigation – regulated sector – all staff

It is an offence to disclose that an investigation into a money laundering offence is being, or may be, carried out if such disclosure is likely to prejudice the investigation. The offence can only be committed if the information on which the disclosure is based came to the person in the course of business in the regulated sector and the offence can be committed even if a person is unaware that a SAR has been submitted.

S342 - All Sectors - Prejudicing an investigation
S342 was amended by Paragraph 8 of TACT and PoCA Regulations 2007. The offence in 342 (2) (a) only applies to those outside the regulated sector. The offence in S342 (2) (b) applies to all persons:

S342 (2) (a) - Non-regulated Sector - Prejudicing a confiscation, civil recovery or money laundering investigation - any staff
This offence applies to the non-regulated sector and relates to the offence of a person disclosing knowledge or suspicion that an investigation is being or about to be carried out and that such disclosure is likely to prejudice an investigation.

S342 (2) (b) - All Sectors - Falsification, Concealing, Destruction of records - any staff
Any person will commit an offence under S342 (2) (b) if he/she falsifies, conceals, destroys, otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents relevant to the investigation unless he/she does not know or suspect that the documents are relevant to the investigation or he/she does not intend to conceal any facts disclosed by the documents from any appropriate officer carrying out the investigation.

S342 – Defences – All sectors
A person does not commit an offence under S342 if:

- he/she does not know or suspect that such disclosure is likely to prejudice an investigation;
- the information on which the disclosure is based came to the person in the course of a business in the regulated sector;
- the disclosure is made in the exercise of a function under the Proceeds of Crime Act 2002;
- he/she is a professional legal adviser and the disclosure is either to a client (or client representative) of the professional legal adviser in connection with the giving of legal advice to the client or to any person in connection with legal proceedings or contemplated legal proceedings, provided that a disclosure is not made with the intention of furthering a criminal purpose.

4.1.4 Permitted Disclosures
Certain disclosures to parties other than SOCA are permitted and which will not result in an offence under S333A. The disclosures must fall within the following categories:

- S333B - disclosures within an undertaking or group, including disclosures to a professional legal adviser or relevant professional adviser;

- S333C - disclosures between institutions, including disclosures from a professional legal adviser to another professional legal adviser;
- S333D - disclosures to your supervisory authority, i.e. FSA.

S333D, permission to disclose to a person's supervisory authority, means that the regulated sector e.g. members' agents and life syndicates, may make a disclosure to the FSA as a supervisory authority, if required.

In addition, whilst Lloyd's is no longer listed as a Supervisory Authority under PoCA, a disclosure by the non-regulated sector (managing agents) to Lloyd's for the purposes of reporting a suspicious transaction to SOCA will not trigger the tipping off offence of prejudicing an investigation (see S342 (2) (a) (p12)), as the disclosure to Lloyd's will be in advance of any money laundering investigation conducted by the authorities.

Where a SAR has already been made and further enquiries are necessary, great care should be taken to ensure that the subject of the disclosure does not become aware that his/her name has been brought to the attention of the authorities. Lloyd's MLRO is available for consultation where there is uncertainty on how to proceed.

The JMLSG advises that where insurers have filed a consent request (see below) and SOCA are making enquiries, and if the insured files a complaint with the Financial Ombudsman because of the delay, it is permissible to notify the Ombudsman's legal team who will liaise with SOCA as appropriate without notifying the insured of SOCA's own investigation. The Ombudsman, once notified of a SAR to SOCA, is also subject to the tipping off offence under PoCA.

4.1.5 S336 - Obtaining consent to proceed with a transaction

If a disclosure involves a transaction, not yet carried out, and which is suspected to involve suspicious activity, then consent can be requested from SOCA to proceed with the transaction (if required). This is known as an "authorised disclosure". Appropriate consent to proceed with a transaction can be provided by Lloyd's MLRO but only where a disclosure has been made by him to SOCA and:-

- SOCA's consent has been obtained; or
- 7 working days have expired without a response being received from SOCA; or
- Consent has been refused by SOCA but a further 31-day period has expired without notification that law enforcement has taken further action to restrain the transaction.

All MLROs will commit an offence under s.336 if they give consent to an employee to carry out a prohibited act (i.e. a primary money laundering offence) if they do not obtain consent from SOCA in accordance with the above requirements.

All disclosures and consent requests can be made to Lloyd's MLRO (see section 6 for guidance) for onward transmission to SOCA.

If SOCA deems that consent is not applicable but that the already submitted disclosure can be treated as a standard SAR, known as a "protected disclosure", then managing/members' agents should record the decision and the reason given. See section 6, Reporting Suspicious Transactions for the definition of a protected disclosure.

4.1.6 Penalties

The primary offences (sections 327, 328 or 329) carry a maximum penalty of 14 years imprisonment or a fine or both on conviction on indictment; and on summary conviction, a maximum imprisonment of 6 months or a fine or both.

The disclosure and tipping off offences carry a maximum penalty of 5 years imprisonment on conviction on indictment and again on summary conviction, a maximum of 6 months imprisonment.

Staff in the non-regulated sector should note that by failing to disclose a suspicious transaction to their MLRO, even though they are not subject to any disclosure offence, they could still face an offence of money laundering if the non disclosure itself facilitates a money laundering transaction. In such circumstances, the penalty they would face would be a maximum of 14 years imprisonment for committing a primary offence, and not the 5 years they would have faced for a disclosure offence.

4.2 THE MONEY LAUNDERING REGULATIONS 2007

The Regulations ensure that UK legislation is in line with European law and firms have adequate and proportionate measures in place to detect, discourage and disrupt money laundering and terrorist financing.

4.2.1 Application of the Money Laundering Regulations 2007

The Regulations (as per the 2003 Regulations) apply to life syndicates and members' agents. General insurance falls outside the regulated sector identified by the 2007 Regulations and the majority of managing agents will therefore not fall within the requirements. However, Lloyd's expects that managing agents apply the provisions of the Regulations as best practice, wherever possible and practicable.

4.2.2 Requirements of the Money Laundering Regulations 2007

In brief, the Regulations implement the following:

Customer Due Diligence

The Regulations go beyond the requirements of the 2003 Regulations, which simply required firms to "identify" customers, imposing more detailed requirements for customer due diligence ("CDD").

CDD requires firms not only to verify the identity of the customer on the basis of reliable and independent documentation but also where applicable to identify and verify the identity of any beneficial owner to obtain information on the purpose and intended nature of the business relationship.

Application of Customer Due Diligence – Risk Based

The 2003 Regulations required CDD to be applied when "establishing a business relationship" or "carrying out an occasional transaction" where there is doubt about the adequacy or veracity of previously obtained information or where there is a suspicion of money laundering or terrorist financing. The Regulations impose a new requirement to also apply CDD measures to existing customers on a risk based approach. Significantly, the Regulations give firms scope to determine the extent of CDD measures on a risk sensitive basis, depending on the type of customer, business relationship, product or transaction. However, a firm must be able to demonstrate to its supervisory authority that the extent of CDD measures is appropriate in view of the risks of money laundering and terrorist financing.

If designed correctly, an effective risk based approach can be a commercial advantage. Ensuring that the right questions are asked for example, at inception of a policy or payment of a claim and good monitoring is in place to spot potential problems, this may avoid cost implications on remedial action/investigation.

Where CDD measures cannot be complied with, a regulated sector firm (e.g. a members' agent or life syndicate) must ensure that a relationship with the customer is not established, or must terminate the transaction/relationship if already established, and consider reporting the matter to SOCA.

Simplified CDD – for lower risk clients

The regulations introduce a new concept of "simplified CDD". In fact, under this measure, a firm does not have to apply CDD measures (unless there is suspicion of money laundering or terrorist financing) where there are reasonable grounds for believing that the customer, transaction or product falls within certain categories. These include customers who are credit or financial institutions subject to the requirements of the EU's Third Money Laundering Directive (or a non-EEA institution subject to an equivalent regime), companies listed on a regulated market in an EEA state (or non EEA equivalent) and certain life insurance products. Part II, Sector 7 of the JMLSG Guidance provides more information about the categories of life insurance policies and their risk level. The EU has recently issued a list of non-EU countries whose AML and CTF systems can be considered as equivalent to EU members. The list can be found on HM Treasury's web site. See Appendix 2 for the relevant link.

Enhanced CDD – for higher risk clients (including Politically Exposed Persons)
The Regulations introduce a further concept of "enhanced CDD" which includes enhanced ongoing monitoring, on a risk-sensitive basis, in any situation where there is a perceived high risk of money laundering and:

- where the customer has not been physically present for identification purposes; or
- in respect of a business relationship or occasional transaction with a politically exposed person ("PEP").

Enhanced due diligence includes measures to obtain supplementary documents, information, data and certification of a customer's identity to mitigate the increased ML risk. Further examples of the measures to apply in these circumstances are set out in the Regulations (Part 2 section 14).

Schedule 2 of the Regulations broadly defines a PEP as someone who holds (or has held in the last year) a prominent public function e.g. heads of state, local government officials with autonomous powers if overseas, members of parliaments, the judiciary, ambassadors etc, which could provide opportunities for making profits from corruption. It also applies to family members and known close associates.

The risk of money laundering with clients who are PEPs may be higher than with other categories, although clearly not all PEPS will be perceived as a threat**.** The Regulation requires firms to:

- Have appropriate risk based procedures to determine whether a customer is a PEP;
- Obtain appropriate senior management approval for establishing or maintaining business relationships with such customers;
- Take reasonable measures to establish the source of wealth and source of funds of such customers;
- Conduct enhanced ongoing monitoring of the business relationship.

The JMLSG Guidance 2007 discusses the PEPs requirements in Part 1, Chapter 5, Section 5.5.

The FSA undertook an exercise in 2006 to assess the systems and controls of a small number of firms, falling within the Wholesale area, in relation to PEPs. In addition to the recommendations above, they noted some additional good practice tips such as:

- Providing PEP-specific training for staff;
- Maintaining PEP account lists (to include if an existing customer becomes a PEP);
- If PEP databases are used, ensure users set correct search parameters and use the most up to date lists, and ensuring that, if a function is outsourced, then up to date lists are used;
- Ensuring that any internal audit reviews consider the PEP risk facing the firm;

- Holding regular forums to discuss systems and controls over PEP risks.

4.2.3 Ongoing Monitoring

Firms must also conduct ongoing monitoring of any established business relationship to ensure that transactions are consistent with the customer's business and risk profile and that data, information and documentation is kept up to date for the purpose of applying CDD measures.

4.2.4 Reliance on third parties for CDD

The Regulations allow firms to rely on certain other third party firms for customer identification and verification (e.g. UK credit/financial institutions authorised by the FSA or accountants and lawyers who are members of the professional supervisory bodies) as long as the third party consents to their evidence being used. Notwithstanding the use of third parties, the firm requesting the CDD remains liable for any failure to apply CDD measures. Section 17 of the Regulations defines the categories of person who may be relied upon.

4.2.5 Record keeping, Systems, Internal Reporting Procedures & Training

The Regulations impose requirements for record keeping, systems, internal reporting procedures and training which are broadly in line with the 2003 Regulations. The JMLSG Guidance provides detailed best practice on compliance with these areas and there is also discussion within this bulletin of these issues at sections 6, 11 and 12.

4.2.6 Supervisory Authorities

The Regulations also clarify the duties that supervisory authorities, such as the FSA, must undertake to ensure that their regulated firms remain compliant with the Regulations. HM Treasury has committed to a post implementation review of the 2007 Regulations to establish whether they are having the intended effect and/or require amendment. The review will be completed by December 2009.

In March 2008 the FSA published a guidance paper entitled "Review of Firms' Implementation of a risk-based approach to anti-money laundering (AML)." The guidance resulted from a survey/review of a selected numbers of firms across the financial services industry. The guidance is posted on the FSA's web site www.fsa.gov.uk at the following link: http://www.fsa.gov.uk/pubs/other/jmlsg_guidance.pdf

4.3. TERRORISM ACT 2000 (TACT)

TACT prohibits involvement in facilitating, financing, possessing or using funds to finance terrorism, as per section 18 of TACT which states that a "money laundering" offence is committed if a person:

"…*enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property by concealment, removal from the jurisdiction, by transfer to nominees or in any other way*".

This offence is applicable to any person within the UK. It is a defence for a person charged with the above offence to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

The United Nations Security Council imposed anti terrorism measures in 2001 on all states to prevent acts of terrorism worldwide. They serve to deny all forms of financial support for those who participate in terrorist acts, and provide safe havens and support for terrorists; and require governments to share with other governments any information about any groups practising or planning terrorist acts. Consequently, a consolidated list of suspected terrorists is available on HM Treasury's website, whose web address is listed at Appendix 2.

4.3.1 Disclosure of Information: Duty

TACT also imposes a disclosure obligation on a two tier basis, with different obligations applying to the regulated and non-regulated sector. The definition of the regulated sector is the same as under PoCA, and therefore the majority of underwriting agents will fall within the non-regulated sector if conducting general insurance business only. Life syndicates and members' agents will fall under the regulated sector.

Section 19 of TACT sets out the disclosure requirements for the non-regulated sector. There is a general duty on a person to report to the firm's MLRO, as soon as is reasonably practicable, any belief or suspicion that a person has committed an offence under section 18. This duty applies to any person where the information came to his attention in the course of a trade, profession, business or employment and is thus applicable to managing agents.

The legal obligation on the regulated sector to submit suspicious activity reports in relation to terrorism is set out at Section 21A of TACT (as inserted by the Anti-terrorism Crime & Security Act 2001 under Schedule 2, part 3, 5 (2)). A person in the regulated sector commits an offence if he/she knows or suspects or has reasonable grounds for knowing or suspecting that another person has committed an offence under section 18 and that this information came to him/her in the course of a business in the regulated sector. He or she must disclose the information as soon as is reasonably practicable.

4.3.2 Penalties

Similar to PoCA, the money laundering offence under TACT (section 18) carries a maximum penalty of 14 years imprisonment, whilst the disclosure offences on conviction carry a maximum penalty of 5 years imprisonment.

4.4. FSA HANDBOOK PROVISIONS UNDER SYSC 3.2.6

On 1 March 2006 the FSA replaced its Money Laundering Sourcebook with high-level provisions in its handbook under its SYSC rules. The section for systems and controls in

relation to compliance, financial crime and money laundering is set out under SYSC rules 3.2.6. SYSC rules 3.2.6A – 3.2.6J are not applicable to all insurance firms but the general provision under SYSC 3.2.6 is, as discussed below.

The provisions reflect the FSA's focus on risk management, systems and controls and the desire to encourage a more flexible, risk-based approach to AML safeguards in firms and to place emphasis on the fact that senior management must take responsibility for implementing AML regimes.

The scope of the SYSC AML requirements is the same as it was for the Money Laundering Sourcebook in that it does not extend to general insurance. Thus for FSA purposes, managing agents are not caught by the SYSC AML requirements in relation to their general insurance business, nor are they caught if they carry out either of the following additional activities:

- Insurance mediation activity in relation to a general insurance contract or pure protection contract;
- Long term insurance business which is outside the Consolidated Life Directive.

They are however subject to the general provision in SYSC 3.2.6 which requires firms to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime.

However, as before, life assurance and the activities of members' agents are additionally caught by SYSC 3.2.6A to 3.2.6J and such entities must comply with the provisions. With regard to general insurance Lloyd's proposes to retain its existing approach, in recognition of the reputational risk of financial crime, and therefore expects managing agents, wherever practicable, to follow all the principles of SYSC's AML requirements.

The SYSC provisions require that firms have systems and controls enabling them to identify, assess, monitor and manage money laundering risk and which are comprehensive and proportionate to the nature, scale and complexity of its activities. These systems should include:

- Training;
- Management Reporting;
- Documentation of risk management policies; and
- Measures to ensure that Money Laundering risk is considered in day to day operations.

4.5 2007 JOINT MONEY LAUNDERING STEERING GROUP ("JMLSG") GUIDANCE [2]

The JMLSG Guidance advises firms on how to meet their legal and regulatory obligations for AML and CTF under the Regulations, PoCA and TACT 2000. Its aim is to promote good practice in countering money laundering and to give practical assistance in interpreting the regulations. The JMLSG Guidance is formally approved by HMT under relevant legislation and is explicitly referred to in the FSA's Handbook. This means that a court or the FSA will take into account whether a firm has followed this guidance.

The Guidance provided by JMLSG is in two parts. The first part [3] is generic guidance, whereas part two [4] is industry sector specific and sector 7 will be useful reading for life syndicates and members' agents.

It gives firms discretion as to how they comply with AML legislation and regulations and which procedures to implement for this purpose but is not intended to be a checklist of steps to take. Firms and employees are encouraged to take a risk based approach as they carry out their duties within the legal and regulatory framework and maintain systems and procedures which are appropriate and proportionate to the risks identified.
The Guidance specifies which statutory and FSA regulatory requirements are mandatory. It also identifies those requirements which must be satisfied but where this may be achieved by a variety of means.

Departure from this guidance and the reason for doing so should be documented and regulated sector firms must be prepared to justify their decision to their supervisory authority.

5. MONEY LAUNDERING REPORTING OFFICERS ("MLROs")

Lloyd's requires each underwriting agent to appoint an MLRO to act as the focal point for all activity relating to money laundering, regardless of whether the underwriting agent is conducting general insurance or regulated business. The MLRO is responsible for implementing effective AML procedures, monitoring compliance with procedures and reporting annually to the Board. FSA approval will be required for MLROs responsible for PoCA regulated sector activities and therefore most managing agents' MLROs will not require approval. However we recognise that most MLROs will hold compliance officer status and have already obtained FSA approval.

It is important that a MLRO has an appropriate level of seniority within the organisation, understands the AML legislation and regulation and has the full support of the Board in carrying out his responsibilities.

---

[2] http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=751&a=11454
[3] http://www.jmlsg.org.uk/content/1/c6/01/14/56/Part_I_-_HMT_approved.pdf
[4] http://www.jmlsg.org.uk/content/1/c6/01/14/57/Part_II_HMT_approved.pdf

6. REPORTING SUSPICIOUS TRANSACTIONS

Please note that the requirement to disclose extends to transactions which have been turned away under the legislation or not fully completed due to suspicious circumstances. A disclosure in this situation is known as a "protected disclosure".

A SAR is treated as a protected disclosure under S337 of PoCA if 3 conditions are satisfied, those being that the information/matter disclosed came to the person making the disclosure in the course of his/her trade or profession, business or employment; that the information/matter causes the discloser to know or suspect or have reasonable grounds for knowing or suspecting that another person is involved in money laundering and; that the disclosure is made as soon as practicable.

It is essential that each underwriting agent has in place procedures to ensure that any suspicion or knowledge of money laundering is reported internally to its MLRO and that this information is passed in turn to SOCA (via Lloyd's if appropriate).

Underwriting agents' disclosure requirements should be satisfied by making a report to Lloyd's MLRO, Sean McGovern, who has delegated the function to the International Regulatory Risk team. This can be achieved by reporting directly to Andy Wragg and to mlro@lloyds.com.

As before (see 4.1.4) a disclosure made via Lloyd's will not constitute a tipping off offence.

Some managing agents have adopted their own internal suspicious transaction reporting forms for employees to complete and return to the MLRO. The following is useful information to capture where possible for submission to Lloyd's or SOCA:

- Subject details, including unique identifiers such as date of birth/NI number/email address/residential address;
- Associated subject's details as above;
- Risk Details – description, value, status (e.g. declined);
- Reason for suspicion

In cases where it is decided not to make a disclosure, a file note should be made by the MLRO outlining the reasons for not doing so. It may be that, as time goes by, a succession of more minor issues may arise, which together give sufficient grounds to make a disclosure.

7. CLAIMS FRAUD

If a claim has been declined because it is deemed to have been made fraudulently, there is no requirement to report the transaction as suspicious, although disclosure of fraud to the Police may still be made. If however a claim is suspected of being fraudulent but there is no

evidence to decline it, we have been advised that managing agents should request consent from SOCA to pay it.

8. LLOYD'S INVOLVEMENT IN REPORTING SARS

SOCA and the FSA have confirmed that the current reporting framework, where Lloyd's submits SARs to SOCA on behalf of the Lloyd's market, is effective and adds value. However Lloyd's and managing/members' agents are responsible to ensure that PoCA reporting obligations are fulfilled.

Managing/members' agents are at liberty to report SARs directly to SOCA without Lloyd's intervention. Lloyd's involvement does however maintain standards and allows trends to be recorded by Lloyd's, which assist in training. It should be recognised that a small element of risk exists in the current reporting structure whereby managing/members' agents should be mindful of reliance on a third party, e.g. Lloyd's, to report on a timely and comprehensive basis, particularly where a consent request has been made and the possibility (albeit unlikely) of failure by Lloyd's to report.

Lloyd's does not filter or alter any referrals made to it by managing/members' agents, but reports them in a timely manner to SOCA based on the agent's decision to report. Lloyd's also reports SARs and consent requests within the required timescales and ensures that agents are aware of the reasons why consent requests are not applicable, or of other comments from SOCA, so that this information can be recorded by the agent as part of its AML controls.

As mentioned under Section 4.1.4, a disclosure by the non-regulated sector (Managing Agents) to Lloyd's for the purposes of reporting a suspicious transaction to SOCA will not constitute tipping off.

Lloyd's is able to facilitate discussions with SOCA to allow managing/members' agents to be guided on the quality of information provided for the purposes of making SARs and also provide any feedback.

Lloyd's has previously invited the Money Laundering Investigation Unit of the City of London Police to present feedback to the Lloyd's market on the type of investigations it carries out as a result of SARs and will continue to provide a regular forum for such events. The Regulations have made it a requirement that the public sector publish statistics on the effectiveness of SARs and feed back to the financial sector on threats and vulnerabilities of money laundering and terrorist financing and on the SARs themselves.

9. RECOGNISING SUSPICIOUS TRANSACTIONS

We have set out below factors which may give rise to a suspicion. This list is not exhaustive and some examples may not be appropriate to certain sectors or classes of business.

In conducting a money laundering risk analysis we would recommend that underwriting agents consider the Money Laundering and Terrorist Financing Typologies published by the Financial Action Task Force ("FATF"). (See Appendix 2)

9.1 New Business

The following situations may generate a suspicion about a new client:

- Difficulties and delays in obtaining copies of accounts or other documents of incorporation, where required, about a new corporate/trust client.
- Reluctance to provide any information or provision of information in general or about the ownership of a risk which is difficult for the underwriting agent to verify.
- Numerous use of offshore accounts, companies/structures in circumstances where the client's needs do not support such economic requirements.
- No discernible reason for seeking the insurance in question, e.g. clients whose requirements are not in the normal pattern of business or the insurance requested.
- Transactions involving third parties, whose involvement becomes apparent at a later stage.
- The client shows no interest in the performance /general terms of his policy but is interested in the early cancellation of the contract.
- Transactions which have no apparent purpose, make no obvious economic sense and appear unrealistic, illegal or unethical.
- A request to insure goods, assets etc, in transit to or situated in countries where terrorism, the production of drugs, drug trafficking or an organised criminal activity may be prevalent or which are the subject of Financial Action Task Force warning notices or on their Non Cooperative Countries and Territories list or on the Transparency International Corruption Perceptions List (see Appendix 2).

9.2 Payment

Large and unusual payments (including insurance premiums and injections of new money into a member's funds at Lloyd's ("FAL") may indicate that further due diligence is required, such as:

- The client purchases policies for an amount which is considered to be beyond his apparent means.

- Overpayment of premium / new money into FAL, with a request to pay the excess to a third party [5] or in a foreign currency.

- Attempts to use a third party cheque when purchasing a policy or payment in cash when the type of business transaction in question would normally be handled by cheques, credit or debit cards or other methods of payment.

9.3 Intermediaries/Brokers

There are many reasons for a client to use an intermediary and for underwriters to deal via intermediaries. The use of intermediaries does however introduce further parties into the transaction, thus increasing opacity and making it possible that the customer's identity and activities are unclear to the insurer. It is therefore important that underwriting agents understand how business is being procured, including the identity of all intermediaries in the placing chain. The following situations may give rise to suspicions and may warrant further enquiry:

- Unnecessarily complex placing chains.

- Excessive commission paid to an intermediary or the involvement of an intermediary whose role appears superfluous.

- The overseas intermediary is based in a jurisdiction which has ineffective, poorly enforced or no money laundering legislation.

- Results of an audit which reveals premium financing arrangements between insureds and intermediaries, which may obscure source of funds or large unusual cash payments.

9.4 Abnormal transactions

- Money passing through a number of different persons and entities may introduce numerous layers to a transaction to create opacity and disguise the source of funds.

- Assignment of a policy to an apparently unrelated third party.

- Early cancellation of policies in circumstances which appear unusual or occur for no apparent reason.

- Cancellation of the policy and a request for the refund to be paid to a third party.

[5] Lloyd's Market Services ("MS") operates its own restrictions concerning third party payments from FAL. In addition, any existing Member providing **directly** to MS notification of a change of bank account details, for instance in respect of interest or dividend payments, must provide copy evidence that the bank account and beneficiary account name correspond to that of the Member i.e. provision of a copy paying-in slip.

- Transactions not in keeping with the normal practice in the class of business to which they relate, e.g. due to nature, size, frequency etc.

- For personal lines business, a number of policies taken out by the same insured for relatively small premiums (normally paid with cash) which are then quickly cancelled, possibly with the return premium requested to be paid to a third party.

9.5 Claims

The claims process could be used in the layering and/or integration stage of the money laundering process. The following situations may give rise to suspicions in this context.

- Claims requested to be paid to persons other than the insured.

- For personal lines sector, apparently legitimate claims that occur with abnormal regularity e.g. regular small claims within the premium limit from the same insured or intermediary.

- A change of ownership/assignment of the policy just prior to a loss occurring.

- Abnormal loss ratios for the class of risk bound under a binding authority, especially where the intermediary has claims settling authority (possible evidence of claims being fabricated and reported to underwriters, or under-reporting of claims where the intermediary is acting as unauthorised insurer, or even not paying claims).

- Claims investigations which uncover evidence of other suspicious activity independent of the claim. For example, the claims investigator might discover that the claimant enjoys a lifestyle which is beyond his apparent financial means or that the insured has not been paying tax or even national insurance income.

10. WRITTEN PROCEDURES TO COMBAT MONEY LAUNDERING

All underwriting agents should adopt written procedures to cover the following:

- Recognition and reporting of suspicious transactions;
- Staff training and awareness; and
- Record keeping.

In order to devise a suitable policy, underwriting agents should identify and record their own business risks by assessing:

- The risks posed by the products they offer;
- The channels through which business is conducted; and
- The countries in which business is done.

A firm should also review its internal money laundering procedures but particularly in relation to:

- Assessing the extent of operational changes and their ML impact, if any;
- Ensuring recommendations from any previous reviews are implemented;
- Reviewing the level of understanding of, and compliance with, training issued to staff;
- Providing further enhancements to ML procedures if required.

11. STAFF TRAINING AND AWARENESS

Managing/members' agents should have appropriate ongoing training to ensure that relevant staff are aware of the basic requirements of the law and the firm's own internal policies to identify and deal with suspicious transactions. The training should be aimed at improving staff understanding and awareness of money laundering and to emphasise their individual responsibilities under AML legislation.

Training should be provided as often as necessary to address movement of employees within the firm and staff turnover and it is recommended that this should occur as a minimum every 2 years. The method of delivery of training and information is not set and will vary according to the size of the agent and the nature of its operation.

Some firms have adopted desk based E-Learning on AML training which can be tailored to different business sectors.

Underwriting agents should ensure that all training and provision of information to staff is properly documented and records retained.

12. RECORD KEEPING REQUIREMENTS

Records must be retained for 5 years from the date on which the transaction was completed or declined. This is an essential component of the audit trail process. If law enforcement agencies investigating a money laundering case cannot link criminal funds passing through the financial systems with the original criminal money, confiscation of the laundered funds and prosecutions may be difficult.

13. STATISTICS

We have listed some statistics relating to the type of suspicious transactions reported to Lloyd's, which might assist underwriting agents in identifying areas of their business which are vulnerable to money laundering.

In 2006 and 2007, 130 SOCA referrals were made by Lloyd's MLRO. Of these, 105 referrals were referred by market participants and the statistics for these are as follows.

- 9% of referrals related to reinsurance coverage, specifically suspicions about the reinsured such as premium concerns, doubts of authenticity and handling of claims.

- 65% of cases related to specie/fine art coverage including vault insurance or goods in transit, e.g. storage of cash, precious metals, copper, selenium and coverage of fine art/gemstones. This figure has been broken down as follows:

    - Over-inflated value of goods - 32%
    - Ownership doubts - 10%
    - Doubts over existence of the property - 9%
    - Coverage being requested to secure a line of credit - 14%

- 4% of referrals were about concerns over the location of the risk.

- 12% of referrals were over doubts of the bone fides of the insured.

- 10% of cases related to other matters, including theft by third party intermediaries, bogus and suspicious claims, tax evasion and concerns over return premiums.

It is stressed that this is not an exhaustive list, nor definitive guidance concerning the matters which warrant referral.

If you have any questions on this guidance please contact Andy Wragg on 020 7327 6387 or at andy.wragg@lloyds.com or Rachael Connor on 020 7327 6380 or at rachael.connor@lloyds.com

APPENDIX 2

SOURCES OF INFORMATION ON MONEY LAUNDERING

Financial Action Task Force on Money Laundering (FATF)
FATF/GAFI
2, rue André Pascal
75775 Paris Cedex 16
France
Website: http://www.fatf-gafi.org

The FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering. This website has links to the FATF's 40 recommendations and 9 Special recommendations document, which consists of evaluation reports, assessing a country's compliance with AML regimes.

On 28 February 2008, FATF issued a statement regarding concerns over the AML/CTF policies of 6 territories. This statement is available at: http://www.fatf-gafi.org/dataoecd/16/26/40181037.pdf

Financial Crimes Enforcement Network (FinCEN)
Website: http://www.fincen.gov

FinCEN is part of the US Department of the Treasury and is a network to share information to combat money laundering internationally and domestically.

The Financial Services Authority (FSA)
25 The North Colonnade
Canary Wharf
London
E4 5HS
Website: http://www.fsa.gov.uk

A link to the SYSC requirements can be found at:

http://fsahandbook.info/FSA/html/handbook/SYSC/3/2

HM Treasury
The Correspondence & Enquiry Unit
2/W1
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ
Website: http://www.hm-treasury.gov.uk

The link to those non-EU countries considered by the EU to have AML and CTF systems equivalent to EU members can be found at:

http://www.hm-treasury.gov.uk/documents/financial_services/money/fin_crime_equivalence.cfm

Lloyd's
Contact details for Lloyd's MLRO are as follows:

Sean McGovern

Telephone:	020 7327 6142
Facsimile:	020 7327 5414
Email:	mlro@lloyds.com

For reporting:

Andy Wragg

Telephone:	020 7327 6387
Facsimile:	020 7327 5988
Email:	mlro@lloyds.com

The International Association of Insurance Supervisors (IAIS)
Website: http://www.iaisweb.org

The IAIS represents insurance supervisory authorities of 180 jurisdictions and has published some useful guidance on anti-money laundering issues.

Joint Money Laundering Steering Group (JMLSG)
Pinners Hall
105-108 Broad Street
London
EC2N 1EX
Website: http://www.jmlsg.org.uk

The website is a service provided by the British Bankers' Association on behalf of JMLSG and contains important information about countering money laundering. The JMLSG Guidance is set out on the web site and can be found at the following links:

http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=751&a=11454
http://www.jmlsg.org.uk/content/1/c6/01/14/56/Part_I_-_HMT_approved.pdf
http://www.jmlsg.org.uk/content/1/c6/01/14/57/Part_II_HMT_approved.pdf

Office of Public Sector Information (OPSI)
Website: http://www.opsi.gov.uk

Operating within OPSI, Her Majesty's Stationery Office (HMSO) is responsible for the publication of legislation and the full texts of PoCA, TACT and the 2007 Regulations can be found on the legislation section of this site.

The Serious Organised Crime Agency (SOCA)
PO Box 8000
London
SE11 5EN
Website: www.soca.gov.uk

SOCA peforms the function of receiving and analysing the suspicious transaction reports it receives from the financial sector and disseminates these to law enforcement authorities.

Transparency International
Website: http://www.transparency.org

Transparency International is a worldwide coalition to address anti-corruption issues and reforms, comprising representations from governments, civil society, business and media. It produces a list of countries ranked by perceived levels of corruption called the Corruption Perceptions Index (CPI).