Money laundering

Definition of “money laundering”

Money laundering is the term used to describe the techniques, procedures or processes used to convert illegal funds obtained from criminal activities into other assets in such a way as to conceal a fund’s true origin so it appears the money has come from a legitimate or lawful source.

In Europe, money laundering is a criminal offence that currently carries a potential prison sentence in the UK of fourteen years. More relevant to the insurance market, assisting and, in certain circumstances, failing to report suspicions of money laundering are criminal offences, punishable by imprisonment. Money laundering funds are deemed to be the proceeds, directly or indirectly, of some activity that is a crime in the UK.

Money laundering and the law

The current legislative framework for money laundering consists of:

- The Proceeds of Crime Act 2002 (Part 7)
- The Terrorism Act 2000 (sections 18-23)
- The Money Laundering Regulations 2003
- FSA Money Laundering Sourcebook

General insurance is within the scope of the Financial Services and Markets Bill but is not subject to the 2003 Regulations or the FSA Money Laundering Sourcebook. Firms must, however, establish systems and controls to counter the risk that they might be used in connection with a financial crime. Systems and controls should support identification of suspected financial criminal activity and also identify a reporting structure up to and including senior management.

All Members are subject to the Proceeds of Crime Act 2002 and The Terrorism Act 2000. The Proceeds of Crime Act (POCA) covers all types of crime, not just arising from organised crime, terrorism or drugs but other (sometimes more socially accepted) crimes such as tax or customs and excise evasion, credit card, cheque or social benefit fraud. There is also no de minimis level so if the amount is only £10, it still needs to be reported. It will be up to the National Criminal Intelligence Services (NCIS) to decide what to do with the information.

In the case of general insurance, the illegal property might be the insurance premium but might equally be the policy itself, if purchased with laundered money. It could also be the subject matter of the insurance, such as a stolen car, or a car bought with the profits of an illegal immigration racket.
Proceeds of Crime Act 2002

Under the Proceeds of Crime Act 2002, the act of money laundering is defined as concealing criminal property; arranging, by whatever means, the acquisition, retention, use or control of criminal property; or acquiring, using or being in possession of criminal property.

Primary offences

There are three primary offences under the Act and they apply to all insurers and intermediaries, including those involved in general insurance business.

Concealing (s.327)

Where someone knows or suspects that property is a benefit from criminal conduct or it represents such a benefit (in whole or in part, directly or indirectly) then they commit an offence if they conceal, disguise, convert, transfer or remove that criminal property from England and Wales, Scotland or Northern Ireland.

Arranging (s.328)

An offence is committed by a person if they enter into or become concerned in an arrangement which they know or suspect, 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, knowing or suspecting that property is a person’s benefit from criminal conduct (in whole or in part, directly or indirectly) acquires, uses or has possession of the property.

Obtaining consent to proceed with a transaction

Making a report to NCIS

The Proceeds of Crime Act requires that a report be made to the NCIS in a prescribed form (see Appendix 1.)

NCIS will analyse the report and check it against its database for possible related information, prior to passing details on for investigation. The information is then forwarded to the Police or Customs or other appropriate agency.

If an authorised disclosure is made in relation to a suspicious transaction which has not yet been carried out, then consent to proceed with the transaction can be requested from NCIS. Members can proceed with a transaction only where a disclosure has been made to NCIS and:

- NCIS consent has been obtained; or
- seven working days have expired without a response being received from NCIS; or
- consent was refused by NCIS but a 31 day period has expired without notification that law enforcement has taken further action to restrain the transaction.
Where a firm has appointed a Money Laundering Report Officer (MLRO), they will commit an offence under s.336 if they give consent to an employee to carry out a prohibited act (a primary offence) if they do not obtain consent from NCIS in accordance with the above requirements.

**Multiple, low value fraudulent transactions**

The theft of a cheque book, debit card, credit card, or charge card can lead to multiple, low value, fraudulent transactions over a short, medium, or long term. However, the identity of the fraudster is often not known and is unlikely to be discovered; consequently, limited intelligence is available for disclosure. Where a card or cheque is used fraudulently to obtain funds or goods and where there is no knowledge, suspicion, or reasonable grounds for knowing or suspecting:

- the identity of the person who is engaged in money laundering; and
- the identity of the person who committed the offence; and
- the origin of the criminal property that has been obtained

firms can seek authorisation from NCIS to apply for separate reporting procedures for these types of fraudulent transactions. Whilst all incidents of this nature must be reported, the use of a specifically agreed arrangement is not compulsory.

**Please note the requirement to disclose also extends to transactions which have been turned away due to suspicious circumstances.**

**NCIS enquiries/consent**

The receipt of a 'suspicious' report will be acknowledged by NCIS and, in the absence of any instruction to the contrary, a firm will be free to operate the customer's account under normal commercial considerations. However, receipt of an acknowledgment letter does not indicate that the suspicion has been investigated or that it is unfounded.

If the enquiries uncover a crime the investigators will serve a Court Order on the Member to provide the records required as evidence. NCIS will make their own discreet enquiries and their investigation will be confidential. A Member cannot be sued for breach of confidentiality for making a report to NCIS.

Where NCIS give consent, following a disclosure, this provides the staff involved with a defence against a charge of money laundering. It is not intended to over-ride normal commercial judgement and a firm is not committed to continuing the relationship with the customer if such action would place the reporting firm at commercial risk. It is recommended, however, that before terminating a relationship in these circumstances, Members should liaise with NCIS or the investigating officer to ensure the termination does not ‘tip-off’ the customer or prejudice the investigation in any other way.

**Penalties**

A person guilty of the offence of ‘failure to disclose’ is liable, on summary conviction, to: imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum, or to both; or, on conviction: an indictment to imprisonment for a term not exceeding five years, a fine or both.
Failure to disclose may also give grounds to be charged with the offence of money laundering itself which carries a maximum penalty of fourteen years imprisonment in the UK.

Reporting overseas offences

The offence of failing to report that an individual is engaged in money laundering applies to all aspects of money laundering, including money laundering abroad that would amount to an offence if it took place in the UK. The obligation of onward reporting to NCIS, however, applies only when the nominated officer has received a report made by someone working within the UK regulated sector.

'Tipping-off' (ss.333 and 342)

It is an offence for any person, if they know or suspect a disclosure has been made, to take any action likely to prejudice an investigation by informing or ‘tipping-off’ those who are the subject of a disclosure, or anyone else involved, including when a disclosure has been made or that law enforcement authorities are carrying out, or intending to carry out, a money laundering investigation.

Where it is suspected or known that a suspicious transaction report has already been disclosed to NCIS, or a MLRO, and further enquiries need to be made, great care should be taken to ensure that those involved do not become aware their names have been brought to the attention of the authorities.

Data Protection Act

The Information Commissioner has issued guidance which addresses the perceived conflict between the ‘tipping-off’ offence on the one hand, the individual's right of access to his personal data under the Data Protection Act 1998 and, on the other, the obligations on financial institutions.

(See [http://www.hm-treasury.gov.uk/media//9A770/money_laundering.pdf](http://www.hm-treasury.gov.uk/media//9A770/money_laundering.pdf) for further information).

Penalties

A person guilty of ‘tipping-off’ is liable, on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or to both, or, on conviction on indictment to imprisonment for a term not exceeding five years or a fine or to both.

Defences

The three primary offences under the Proceeds of Crime Act have the following ‘defences’ available:

1. An authorised disclosure was made, either under internal arrangements to a MLRO or to a law enforcement authority, before the prohibited act (the transaction) was done, and appropriate consent to proceed was obtained.

A disclosure is authorised if:

(a) the disclosure is to a constable, a customs officer or a nominated officer (the firm’s MLRO); and

(b) the disclosure is made using the NCIS disclosure form
A nominated officer is someone who has been nominated by their employer to receive internal reports of suspected money laundering.

2. The disclosure was made after the prohibited act was undertaken and there was good reason for failing to make the disclosure before the transaction was undertaken and the disclosure was made on an individual's own initiative, as soon as it was practicable for them to do so.

3. The defendant intended to make an authorised disclosure and had a ‘reasonable excuse’ for not doing so.

4. The procedure in question was carried out to enforce the provision of the Act or other relevant Acts relating to criminal conduct or benefit from criminal conduct. (This provision is aimed primarily at police officers and other enforcement agencies taking possession of criminal property pending an investigation/trial).

5. In the case of an acquisition offence (s329) there is an additional defence for someone who acquired, used or had possession of the property for adequate consideration, provided they did not know or suspect the goods or services might help another carry out a criminal conduct. Consideration is regarded to be ‘inadequate’ if it is significantly less than the value of the property received or the value of its use or possession.

For general insurance intermediaries which are not subject to the Money Laundering Regulations 2003, POCA does not impose a statutory duty on someone who is not a ‘nominated officer’ to make a disclosure to an MLRO/NCIS. The primary money laundering offences and the tipping-off offence, however, still apply to all individuals and businesses. If a person knows or suspects, in relation to s.327, s.328 and s.329 (‘prohibited acts’) and does not make a proper disclosure, they will not be able to rely on their ‘unregulated status’ as a defence in a Court of law if they are charged with a primary offence.

**Terrorism Act 2000**

Sections 18 to 23 of the Terrorism Act 2000 refer to the money laundering offences that could be committed in relation to terrorist funding. For example, s.18 states that a person commits an offence if they enter into or become concerned with an arrangement which facilitates the retention, or control by, or on behalf of, another person of terrorist property. An offence, contrary to S.18, would be committed if a person did not know but should reasonably have suspected, the funds involved were terrorist property.

The offences and penalties under the Terrorism Act 2000 are broadly the same as in the Proceeds of Crime Act 2002. A separate area within NCIS handles referrals relating to terrorist activities.
Where is money laundering covered within GISC Rules?

Section F, paragraph 14.1 states that Members agree to observe and comply with “…………any relevant laws………”. This includes The Proceeds of Crime Act 2002 and Terrorism Act 2000.

Practice Requirement G3, paragraph 4.3 requires Members to provide Employees with adequate knowledge of the consequences of money laundering.

Where to find the FSA money laundering rules

Various requirements relating to authorised firms’ anti-money laundering processes and procedures are to be found in:

- PRIN – Principles for Business
- APER – Approved Persons – principles and code of practice
- SYSC – Senior Management Arrangements/Systems and Controls
- TC – Training and Competence

FSA – Principles for Business

At its most basic level, Principle 3 (management and controls) requires that a firm take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management.

Obligations on Approved Persons

For individuals the statements of principle for Approved Persons and the underlying Code of Practice will impose a new level of accountability on those who are Approved Persons and, in particular, those exercising “significant influence” functions, to ensure they act with integrity and with due skill, care and diligence in carrying out their controlled functions.

At a more detailed level, APER 4.7.9 covered by APER 4.7.2 specify behaviour which would not comply with the FSA Statement of Principle 7, Standards for Approved Persons including:

- failure to implement adequate systems and controls
- failure to monitor
- failure to discharge money laundering responsibilities

FSA - Systems and Controls

The requirements in the FSA sourcebook, in relation to systems and controls, require a firm to establish and maintain such systems as are appropriate to its business (SYSC 3.1.IR), as are required for compliance with the regulatory regime and for countering the risk that the firm might be used to further financial crime (SYSC 3.2.6R). For these purposes, financial crime is defined as any offence involving fraud or dishonesty, misconduct in, or misuse of, information relating to any financial market or handling directly or indirectly the proceeds of crime.
Record keeping is also a fundamental requirement and firms must take care to make and retain adequate records (SYSC 3.2.20R) including those for anti-money laundering purposes.

**FSA - Training and Competence**

All firms are expected to make commitments to training and ensure competence so that all staff “associated with” regulated activities are competent; remain competent; are appropriately supervised and their competence is regularly reviewed. This includes training relevant employees in their obligations and in the procedures for recognising and reporting suspicions of money laundering.

**What are some of the typical signs of money laundering?**

The extent to which Members may be a possible target for money laundering will depend on the type of organisation, the activities it engages in and the size of its transactions.

Laundering money is most likely to be attempted by a new customer, using one or more application forms, false names and fictitious companies (although existing customers are not exempt from opportunities). Money launderers will often have large amounts of cash they will attempt to deposit into the financial system. Members should pay particular attention to large or unusual methods of payments of premiums. Whilst many crimes such as drug dealing, generate money in cash - others including fraud and embezzlement, do not.

The use of more than one intermediary introduces further parties into the transaction, creating layers and making it easier for a customer to remain anonymous. Members should conduct, thorough due diligence checks, including the intermediary’s financial status, on any intermediaries they use. It is important for Members to realise they will probably only ever see a small part of the overall picture of money laundering and must be alert to signs that a transaction is part of a much wider process.

**Recognising suspicious transactions**

Members should be able to recognise and report suspicious transactions. This means any matter that comes to their attention, in the course of business, which in their opinion gives rise to knowledge of, or suspicion of money laundering or when reasonable grounds exist for knowing or suspecting another individual is engaged in money laundering.

**What is 'suspicion'?**

Suspicion has been defined by the Courts as being beyond mere speculation and based on some foundation.

**What is 'knowledge'?**

- Actual knowledge;
- Knowledge of circumstances that would indicate facts to an honest and reasonable person.
The law requires Members (inter alia) to be alert to recognising transactions that might be part of a money laundering operation and for funds, or assets, that might be the proceeds of crime or providing support for terrorist activities. A person who considers a transaction to be suspicious would not be expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime.

Members’ knowledge of their customers should help them to decide whether, taking into account what they know about them and their background, the transaction is something unexpected or unusual. Unusual is not necessarily suspicious if there is a legitimate explanation. Members should seek explanations, wherever possible, for suspicious or unusual transactions but they should remember that they must not give any indication to the customer or anyone else they think may be involved in the transaction (‘tipping-off’). It would, however, be quite appropriate to ask for an explanation as to why a policy has been cancelled. A Member could, for example, express concern at the loss of custom and enquire why the customer has decided to cancel. A legitimate explanation may be, for example, that the customer has simply obtained a better quotation with another company.

If there is a suspicion of insurance fraud - even if there is insufficient evidence for an insurer to prove criminal intent and decline a claim or avoid a policy - then under the Proceeds of Crime Act, if that suspicion implies the possibility of money laundering, a report must be made. Accordingly, whilst an insurer may ultimately have to pay a claim, for, say, the loss of a stolen car, which they may suspect is fraudulent, the insurer will still need to make a report to NCIS.

Suspicion can be personal and subjective but it must be beyond mere speculation. In deciding whether, in a particular instance, Members have ‘reasonable grounds’ to know, or suspect money laundering they should consider how it would look to someone else, knowing what they knew, seeing what they had seen? If Members consider that, at some future date, they may not be comfortable with sustaining their original belief that there were no reasonable grounds to suspect money laundering related or other criminal activities, they should make a report.

The following is a list of areas of vulnerability and factors which may give rise to suspicion:

**New business**

- A new corporate/trust client where there are difficulties and delays encountered in obtaining copies of accounts or other documents of incorporation, where required.
- A personal lines customer for whom verification of identity proves unusually difficult and who is reluctant to provide full details.
- A client who is reluctant to provide any information about themselves or their business.
- A customer who provides information which then proves difficult to verify fully.
- The client uses numerous offshore accounts, companies/structures in circumstances where the client’s needs do not support such economic requirements.
- A client with no discernible reason for using the underwriting Member’s service, for example, clients whose requirements are not in the normal pattern of, or are inconsistent with, the Member’s business which could be more easily serviced elsewhere.
- Any transaction involving an undisclosed third party.
• The client shows no interest in the performance/general terms of his policy or suggests that cost is not an issue but is more interested in early cancellation of contract.
• Transactions which have no apparent purpose and make no obvious economic sense.
• A request to insure goods, assets etc. in transit to or situated in countries where terrorism, the production of drugs, drug trafficking or any organised criminal activity may be prevalent.

Payment
• A customer who offers to pay a large premium with cash.
• The client purchases policies for an amount which is considered to be beyond his apparent means.
• A customer who asks to make payments through Bank Giro rather than cheque or direct debit.
• Over payment of premium with a request to pay the excess to a third party.
• Attempts to use a third party cheque when purchasing a policy.
• Payment in cash when the type of business transaction in question would normally be handled by cheques or other methods of payment.
• Where a customer who has always paid by cheque, DDM or credit card, suddenly offers to pay with cash.
• A client who says he is unemployed, or holds himself out as employed but in a low paid occupation, arranging insurance for which he is able to pay a substantial premium.

Intermediaries
• Unnecessarily complex placing chains.
• Excessive profit commission paid to an intermediary who has no apparent involvement in the transaction.
• The unnecessary use of an intermediary in a transaction.
• The overseas intermediary is based in a jurisdiction which, it is understood, has ineffective or no money laundering legislation, or its rules are not vigorously enforced.
• The use of intermediaries introduces further parties into the transaction thus increasing opacity, making it potentially easier for a customer to remain anonymous.

Abnormal transactions
• Assignment of a policy to an apparently unrelated third party.
• Early cancellation of policies in circumstances which generate a large return premium, particularly where they 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 (particularly where cash was tendered).
• Client establishes a large insurance policy and, within a short period of time, cancels the policy and requests the premium to be refunded to a third party.
• Transactions not in keeping with the normal practice of the class of business to which they relate, e.g. due to nature, size, frequency etc.
• A number of policies taken out by the same insured for low premiums (normally paid with cash) which are then cancelled, especially where the return of premium is made to a third party.
• Customers who regularly insure against a common risk and make a series of small claims.
• Customers who make a practice of early cancellation of policies.
• Extensive use of corporate structures and trusts, in circumstances where the client's needs are inconsistent with the use of these structures.

Claims

• Claims requested to be paid to persons other than the insured.
• ‘Legitimate’ claims but they occur with abnormal regularity, e.g. regular small claims within the premium limit.
• 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 cover holder has claims settling authority.

What does GISC expect of its Members?

Any failure to understand the anti-money laundering legislation will leave Members and their employees, whether or not they fall under the regulated sector, vulnerable to investigation and prosecution. The law imposes obligations on employees personally but Members themselves are required to put in place policies, procedures and training to help and protect staff. It is, therefore, imperative that the whole of an organisation, from top to bottom, understand, supports and acts on the new legislation.

Where a Member decides to appoint a MLRO, they must have the capability, and be provided with the resources and support, to make the necessary decisions for their firm and any disclosures to NCIS.

Members will, therefore, be expected to:

• establish and implement policies, procedures and controls to guard against their business being used to launder the proceeds of crime and generally to forestall money laundering and/or terrorist funding;
• have in place systems that ensure that the source of client funds are identifiable;
• ensure staff understanding the awareness of money laundering and the risks of committing a primary or related criminal offence;
• train relevant staff in how to recognise suspicious activity;
• have a procedure in place to record suspicious activities;
• know how and who will report any suspicious activity to The National Criminal Intelligence Service.

All Members should, therefore, adopt written procedures to cover the following:

• recognition and reporting obligations – guidance to staff on the kinds of transactions that might arouse suspicion and what internal reporting is necessary;
• staff training and awareness;
• external reporting to NCIS;
• record keeping.
Written internal policies, procedures and controls should, where appropriate, deal effectively with the threat of money laundering and financial crime within each organisation. In order to devise a suitable policy, Members should identify their own business risks by assessing:

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

**Reporting suspicious transactions**

All staff of Members should report information that comes to their attention in the course of their business activities which, in their opinion, gives rise to knowledge or suspicion of money laundering. The primary money laundering offences and tipping off offences apply to all individuals and businesses.

All suspicions reported to the MLRO or nominated Authority, should be documented (in urgent cases this may follow an initial discussion by telephone). If reports are made by telephone, it is important that the MLRO provides the documentary report and keeps a record of the full name of the member of staff, their internal location within the firm and full details of the transaction, including date and time.

To protect the integrity of employees when reporting suspicions, all telephone calls should be recorded whenever possible, full details of time, date of the call and the reference number or identity of the person receiving the call should be kept in a safe place. Where Members have appointed a MLRO, they will be responsible for deciding whether to make a formal disclosure to NCIS. By lodging their internal report, employees will have completely fulfilled their obligations under the law.

The MLRO, or nominated person, should acknowledge receipt of the report in writing and, at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e. "tipping-off". The employee should also be reminded to ensure that they have a full record of the matter. All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to NCIS, should be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation and the suspicions are confirmed. Following reporting of a suspicious matter, the law enforcement agency may request further information regarding the nature of the suspicion or additional background information.

The reporting of a suspicion in respect of a client or an account does not remove the need to report subsequent suspicions that may arise in respect of the same client. If other suspicious transactions or events occur, whether of the same nature or different to the original suspicion, such new suspicions should continue to be reported to the MLRO or NCIS as they arise.

The national reception point for disclosure of suspicions is the Economic Crime Branch of NCIS.
The Economic Crime Branch is staffed jointly by police and custom officers and its postal address is Financial Intelligence Division, National Criminal Intelligence Service, PO Box 8000, London SE11 5EN. The unit can be contacted during office hours on: **020 7238 8607**. Outside office hours an answer phone operates on that number. Disclosures should be transmitted by post or fax on: 020 7238 8286. The latter method of reporting can give the Member tangible evidence the document has been received by NCIS.

When consent is needed for a transaction which has yet to be carried out, the disclosure should be marked 'CONSENT' and faxed to the NCIS Financial Crime Branch Duty Desk (020 7278 8286) immediately the suspicion is identified. The Duty Officer will then ‘fast track’ the report and carry out the necessary in-house NCIS enquiries, before contacting the appropriate law enforcement agency seeking a 'consent' decision.

NCIS also has a website: [www.ncis.co.uk](http://www.ncis.co.uk).

**Record keeping requirements**

Under the Act, records of transactions **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. Those implicated in the deliberate mismanagement or destruction of such records, with the intent of denying access to the same, in the case of money laundering are, at the least, an accessory to a criminal offence. When a case is reported the investigators may need to follow the movement of funds through many transactions and through different companies. The investigators aim will be to reconstruct the money trail and to identify the parties involved.

The investigating officers will need to know:

- Who were the parties to each transaction?
- Who was the underlying beneficial owner of the funds or policies?
- Whether and, if so, how was the customer's identity verified?
- What precisely happened in the transaction?
- What evidence do you have?

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 cannot be made.

**GENERAL**

**Members should take note that this document is a general purpose advisory summary only** of money laundering in relation to general insurance activities. If Members or their employees have any concerns about money laundering obligations and how they will impact on their business or regarding anti-money laundering systems and processes they should seek expert advice.