An Introduction to the UK Anti-Money Laundering Regime

SLAUGHTER AND MAY
March 2008
## CONTENTS

1. Introduction  
   1.1 Money Laundering  
   1.2 The Regulated Sector  
2. UK Anti-Money Laundering Measures  
   2.1 The Money Laundering Regulations and the FSA Handbook  
   2.2 Substantive Money Laundering Offences  
   2.3 Appropriate Consent  
3. What does this mean in practice?  
4. A practical example  
5. Legal professional privilege  
6. Conclusion  
Appendix – Summary of the Application of Legislative Provisions to Persons Working in Businesses Outside the Regulated Sector
1. INTRODUCTION

The UK’s anti-money laundering regime has evolved considerably since 1993 when the first European-wide attempts to combat money laundering were introduced. Any business or person who comes into contact with the financial system will by now have encountered anti-money laundering measures to some extent – the simplest example of which is the requirement to provide evidence of identity. The interaction of the various legislative and regulatory requirements can be difficult to understand, particularly for those who do not have first-hand experience of applying those requirements.

This memorandum is intended to provide an introduction to the UK anti-money laundering regime for those firms which are not directly subject to the core anti-money laundering legislation (i.e. those which do not operate within the “regulated sector” discussed below) but which are nonetheless affected by the legislation as a result of dealing with businesses which operate within the regulated sector. Also, certain aspects of the UK’s anti-money laundering regime apply to all persons regardless of their involvement with the regulated sector, and those aspects are also explained in this memorandum.

1.1 Money Laundering

It is helpful to understand what is meant by the term “money laundering”. The relevant legislation defines money laundering by reference to the criminal offences which money launderers may commit: the primary statutory offences outlined below, including any attempt, conspiracy or incitement to commit such an offence and any act which constitutes aiding, abetting, counselling or procuring such an offence, and including conduct which would amount to any such offence if it occurred in the UK.1

The common understanding of the term money laundering is that it is the process by which the proceeds of criminal conduct are used, moved or dealt with in such a way as to mask their unlawful origins. The legal reality, however, is that the relevant statutes criminalise not only overt, intentional dealings with the proceeds of crime, but also conduct which can arise simply as a result of a legitimate business coming into contact with criminals and the proceeds of their crimes.

Fundamentally, the UK anti-money laundering regime does not seek directly to prevent crime; rather, it seeks to prevent criminals from enjoying the use of the proceeds of their crime. This objective is in essence achieved by criminalising a person’s involvement with criminals and the proceeds of their crime, and in particular criminalising conduct which might assist criminals to retain, use or otherwise benefit from those proceeds.

1.2 The Regulated Sector

The “regulated sector” for UK anti-money laundering purposes includes all those firms which are part of the financial services community regulated by the Financial Services Authority (the “FSA”), including banks, insurance companies, investment firms and brokers. The regulated sector also

---

1 Refer to section 340 POCA 2002.
includes, among others, lawyers, accountants and tax advisers, those operating foreign exchange or cheque cashing businesses, estate agents and any business which deals in goods where cash payments of €15,000 or more are accepted (such as auctioneers).

The implication of a firm operating within the regulated sector is that the full range of anti-money laundering measures described below will apply to its business.
2. UK ANTI-MONEY LAUNDERING MEASURES

The UK anti-money laundering regime can be divided into two areas: the administrative and regulatory requirements, and the substantive offences. The administrative requirements are set out in the Money Laundering Regulations 2007 (the “2007 Regulations”)\(^2\) and apply only to firms in the regulated sector; in addition, financial institutions which are subject to regulation by the FSA must comply with the FSA’s high-level principles on money laundering\(^3\). The substantive offences, some of which apply only to those in the regulated sector but others of which apply to all persons, are primarily set out in Part 7 of the Proceeds of Crime Act 2002 (“POCA 2002”).

Separate substantive offences relating to dealings with terrorist funds and the financing of terrorism are set out in Part III of the Terrorism Act 2000 (the “Terrorism Act”).

2.1 The Money Laundering Regulations and the FSA Handbook

The 2007 Regulations, which came into force on 15 December 2007, implemented the provisions of the Third EU Money Laundering Directive\(^4\) in the UK. The 2007 Regulations replaced the Money Laundering Regulations 2003\(^5\) with which firms in the regulated sector were previously required to comply.

The purpose of the 2007 Regulations is to impose obligations on firms which provide access to financial services (and other similar services attractive to money launderers) to monitor, and to restrict access to those services, for persons believed to be engaged in money laundering. Accordingly, the 2007 Regulations require that firms in the regulated sector:

- carry out identity checks on potential customers;
- keep records of all relevant interactions with their customers;
- train their employees how to recognise potential money laundering activity; and
- have in place procedures which enable employees to report suspicious activities.

If a firm fails to comply with these requirements, criminal sanctions apply, including fines and up to two years’ imprisonment for directors and senior management.

For firms which are regulated by the FSA, the FSA Handbook is an additional source of anti-money laundering obligations. Neither the 2007 Regulations nor the FSA Handbook have any direct application to firms or individuals outside the regulated sector.

\(^2\) SI 2007/157.
\(^3\) Paragraphs 3.2.6A – 3.2.6J of the FSA’s Senior Management Arrangements, Systems and Controls Sourcebook (SYSC).
\(^4\) 2005/60/EC.
\(^5\) SI 2003/3075.
2.2 Substantive Money Laundering Offences

The substantive money laundering offences are set out in POCA 2002. These serious criminal offences are, broadly speaking, designed to prevent criminals and those involved in assisting criminals dealing in any way with the proceeds of criminal conduct.

(A) Primary Substantive Offences

There are three primary offences, which any person (including a person engaged in business outside the regulated sector) may commit:

- concealing, disguising, converting, transferring the proceeds of crime or removing the proceeds of crime from the jurisdiction;

- entering into or becoming concerned in an arrangement which a person knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of the proceeds of crime; and

- acquiring, using or possessing the proceeds of crime.

As noted above, for these purposes the status of the person engaging in the relevant conduct is irrelevant. Unlike the 2007 Regulations and the FSA Handbook, the provisions of POCA 2002 apply to all legal persons, individual and corporate, irrespective of the nature of their business or whether they are engaged in business at all. Fines can be imposed for these offences not only on corporate entities but also on individual directors, managers and officers; ultimately individuals involved in the commission of a serious money laundering offence can be imprisoned for up to 14 years.

It is important, therefore, to understand what is meant by the proceeds of crime. The statutory concept of the proceeds of crime, or “criminal property” as it is defined in POCA 2002, is very wide. Criminal property is any benefit (monetary or otherwise) from criminal conduct, or any property representing the same (in whole or part and whether directly or indirectly) provided the alleged offender knows or suspects the property is such a benefit. It is immaterial whether the criminal conduct which generated the benefit occurred in the UK or abroad, subject to the condition that if the relevant conduct occurred abroad and was not at the time it occurred unlawful under the criminal law of that country, it must be conduct which would be criminal if it had occurred in the UK and would be punishable in the UK by more than one year in prison.

---

6 Sections 327, 328 and 329 POCA 2002.
7 Section 327, POCA 2002.
8 Section 328, POCA 2002.
9 Section 329, POCA 2002.
The extra-territorial effect of the UK’s anti-money laundering regime can give rise to difficulties for firms which carry on a business overseas. One particularly problematic issue for such firms is the use of “facilitation payments”, which are commonly paid in some jurisdictions (and not necessarily restricted by local law) but which can amount to bribes or corrupt payments as a matter of UK law. The receipt of both the payment and any benefit which accrues in return for the payment may therefore be tainted as criminal property for the purposes of POCA 2002. Any firm which becomes involved with facilitation payments, or with persons who fund, make or receive such payments, must therefore carefully consider its position not only under UK anti-corruption legislation but also under UK anti-money laundering legislation.

It is important to note that there is no de minimis or time limitation in respect of the criminal conduct which can give rise to criminal property. In other words, minimal proceeds from a crime committed any time before the commencement of the relevant legislation can generate criminal property for the purposes of the primary money laundering offences.

Whilst the term criminal property clearly includes the proceeds of, for instance, a fraud or theft, wherever committed, it is perhaps less obvious that the definition could also include any indirect financial benefit which a business receives as a result of minor administrative offences under health and safety legislation, or companies legislation.

It is also worth emphasising that, for each of the three money laundering offences under POCA 2002 described above, a central ingredient of the offence is the knowledge or suspicion of the person concerned that the property is derived from criminal conduct – if the alleged offender does not know or suspect that the property involved is the proceeds of criminal conduct, the offences are not committed.

(B) Secondary Substantive Offences

In addition to the three primary money laundering offences described above, there are also three secondary offences, two of which apply only to firms operating within the regulated sector and one of which applies to all persons. These offences are referred to in this memorandum as secondary offences because they are concerned not with primary money laundering conduct, but rather with a person’s action or failure to act upon discovering potential money laundering. The secondary offences are as follows:

> where a person working in a business in the regulated sector knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is engaged in money laundering (i.e. one of the primary offences described above), but fails to disclose that knowledge or suspicion to a relevant officer; this is known as the “failure to disclose” offence;


 Section 330, POCA 2002.
where a person working in a business in the regulated sector knows or suspects that another person's suspected involvement with money laundering has been disclosed to relevant UK investigatory authorities, or that an investigation into allegations that an offence has been committed is being contemplated or is being carried out, but nonetheless makes a further disclosure to any other person which is likely to prejudice any investigation which might be conducted in light of the original disclosure; this is known as the “tipping off” offence; and

> where a person, whether he works in a business in the regulated sector or the non-regulated sector, knows or suspects that an investigation in connection with alleged money laundering has or is about to be commenced in respect of another person but nonetheless makes a disclosure to any other person which is likely to prejudice any such investigation, or interferes with material which is likely to be relevant to such investigation; this is known as the offence of “prejudicing an investigation”.

These are serious offences. The tipping off offence carries a maximum penalty of two years’ imprisonment; the other two secondary offences carry a maximum penalty of five years’ imprisonment.

Limited defences and exceptions are available but the simplest means for a person to avoid committing a secondary offence under POCA 2002 is to disclose any information giving rise to knowledge or suspicion of money laundering to a relevant officer and to keep confidential the fact of having made that disclosure. A relevant officer means, for these purposes, either the firm’s money laundering reporting officer (the “MLRO”) if it has one – all regulated sector firms are required to appoint an MLRO, but other firms are not – or to the Serious Organised Crime Agency (“SOCA”).

For firms which are not in the regulated sector but which do have an MLRO, it is worth noting that although the failure to disclose offence under section 330, POCA 2002 (described above) does not apply to the non-regulated sector, section 332, POCA 2002 prescribes a similar failure to disclose offence which applies to any MLRO of a firm carrying on business outside the regulated sector.

(C) Terrorism Act Offences

Whereas POCA 2002 applies to dealings with the proceeds of criminal conduct, the Terrorism Act applies to dealings with funds used to finance or otherwise support terrorism. The primary terrorist finance offences are set out in sections 15-18 of the Terrorism Act and are similar but not identical to the POCA 2002 primary offences outlined above:

> inviting, receiving, providing or possessing money or other property intending or having reasonable cause to suspect that it may be used for the purposes of terrorism;

12 Section 333A, POCA 2002.
13 Section 342, POCA 2002.
14 Sections 15 and 16, Terrorism Act.
> entering into or becoming concerned in an arrangement as a result of which money or other property is made available or is to be made available to another and which the alleged offender knows or has reasonable cause to suspect will or may be used for the purposes of terrorism, and

> entering into or becoming 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, transfer to nominees or in any other way.

The primary terrorist finance offences are punishable by fines and up to 14 years’ imprisonment.

Not all of these primary terrorist finance offences require knowledge or suspicion on the part of the offender. Section 18 of the Terrorism Act is a strict liability offence. It is, however, a defence for a person charged with a section 18 offence to show that he did not know and had no reasonable cause to suspect that the arrangements related to terrorist property – crucially, therefore, the alleged offender is required to prove his lack of suspicion in order to rely on the defence.

The secondary offences under the Terrorism Act are similar to those under POCA 2002 but not identical:

> where a person working in a business in the regulated sector knows or suspects, or has reasonable grounds for knowing or suspecting, that another person has committed, or attempted to commit, a terrorist finance offence, but fails to disclose that knowledge or suspicion to a relevant officer, the “failure to disclose” offence;

> where a person working in a business in the regulated sector knows or has reasonable cause to suspect that another person’s suspected involvement with terrorist financing has been disclosed to relevant UK investigatory authorities but nonetheless makes a further disclosure to any other person which is likely to prejudice any investigation which might be conducted in light of that original disclosure, the “tipping off offence”; and

> where a person, whether he works in a business in the regulated sector or the non-regulated sector, knows or has reasonable cause to suspect that another person’s suspected involvement with terrorist financing has been disclosed to relevant UK investigatory authorities but nonetheless makes a further disclosure to any other person which is likely to prejudice any investigation which might be conducted in light of that original disclosure, the “tipping off offence”.

---

15 Section 17, Terrorism Act.
16 Section 18, Terrorism Act.
17 Section 22, Terrorism Act.
18 Section 18(2), Terrorism Act.
19 Section 21A, Terrorism Act.
20 Section 21D, Terrorism Act.
authorities, or that an investigation in connection with alleged terrorist finance offences has or is about to be commenced in respect of another person, but nonetheless makes a further disclosure to any other person which is likely to prejudice any investigation which might be conducted in light of that original disclosure or interferes with material which is likely to be relevant to such investigation, the “prejudicing an investigation” offence\(^\text{21}\).

Again, these are serious offences. The tipping off offence carries a maximum penalty of two years’ imprisonment; the other two secondary offences carry a maximum penalty of five years’ imprisonment.

It is important to note that the Terrorism Act also contains a failure to disclose offence for persons engaged in business in the non-regulated sector. Section 19 of the Terrorism Act sets out a failure to disclose offence in relation to terrorist funds which arises if a person acting in the course of a trade, profession, business or employment outside the regulated sector “believes or suspects” that another person has committed, or has attempted to commit, a primary terrorist finance offence but fails to disclose that belief or suspicion to a relevant officer. Again, it is a serious offence, punishable by up to five years’ imprisonment.

As with the POCA 2002 offences described above, limited defences and exceptions are available but the simplest means for a person to avoid committing a failure to disclose or tipping off offence is to disclose any information giving rise to knowledge or suspicion of a terrorist finance offence to a relevant officer and to keep confidential the fact of having made that disclosure.

2.3 Appropriate Consent

To avoid committing a primary offence under POCA 2002 any person can seek consent from SOCA to engage in a particular activity or course of conduct. If a business, or any of its employees, knows or suspects that a proposed course of conduct could involve the commission of one of the three primary money laundering offences under POCA 2002, it can and should seek appropriate consent by making what is known as an “authorised disclosure” to SOCA\(^\text{22}\). In the case of a firm in the regulated sector, an authorised disclosure to SOCA seeking appropriate consent can be made at the same time as a disclosure which is made to SOCA to avoid committing a failure to disclose offence.

In order not to commit a primary money laundering offence, a business should seek appropriate consent prior to any action being taken or being continued in connection with the suspected money launderer or laundering, and no further steps should be taken in relation to the proposed transaction pending receipt of consent from SOCA.

\(^{21}\) Section 39, Terrorism Act.

\(^{22}\) Section 338, POCA 2002. Authorised disclosures can also be made to a constable or customs officer. The constable or customs officer is required under section 339ZA, POCA 2002 to pass all such disclosures on to SOCA, so SOCA is always effectively the recipient of authorised disclosures.
There are three ways in which consent may be obtained\textsuperscript{23}. SOCA can give its express consent during the period of 7 working days starting after the date of the disclosure. Alternatively if SOCA does not grant consent within that 7 working day period and does not otherwise expressly refuse to grant consent, it is deemed to have been given.

If consent is expressly refused within that period, SOCA then has 31 calendar days from the date of refusal to investigate the subject of the disclosure. Upon the expiration of that 31 day period, and in the absence of express consent or any other interim restraining action, consent is deemed to have been given.

There is a similar consent regime under the Terrorism Act\textsuperscript{24}.

The authorised disclosure route is, in many circumstances, the only practical way forward where a firm has identified a potential money laundering concern of the type highlighted above. It is important to bear in mind, however, that to the extent that consent is obtained, whether express or deemed, it is only granted on the basis of the facts disclosed. Firms should take care, therefore, to ensure that all relevant information is included in an authorised disclosure.

\textsuperscript{23} Section 335, POCA 2002.

\textsuperscript{24} Sections 21 and 21ZA, Terrorism Act. As with the consent regime under POCA 2002, authorised disclosures can be made to a constable as well as to SOCA. However, one slight difference under the Terrorism Act is that where the authorised disclosure is made to a constable rather than to SOCA, there is no provision whereby the constable is deemed to have given consent if no express consent has been granted within a period following the disclosure.
3. WHAT DOES THIS MEAN IN PRACTICE?

It will be evident from the preceding paragraphs that all businesses, and those individuals working in them, must take steps to ensure that they do not become involved in the commission of a substantive money laundering offence. It is also important that, once a person becomes aware of potential money laundering activities, appropriate action is taken to report it (if relevant) and that nothing which is done as a result of that knowledge or suspicion inadvertently gives rise to a tipping off offence.

If the scope of the substantive offences was confined to dealings with the proceeds of the types of crime that are commonly associated with money laundering – drug crime, fraud or theft – that ought not to be difficult for most businesses. Unfortunately, because the UK anti-money laundering regime applies to dealings with the proceeds of any crime, it is not necessarily such a straightforward matter for all businesses.

The wide definition of money laundering described above remains a particular concern as much for firms operating within the regulated sector as for those outside it. Despite lobbying by lawyers and the financial services sector for the introduction of a de minimis threshold test, or to limit further the extra-territorial scope of the money laundering offences, the government has so far largely resisted any narrowing of the definitions – ostensibly because it does not wish to restrict the ability of law enforcement agencies to pursue criminal property wherever it arises.

Firms operating outside the regulated sector should also appreciate that the financial institutions and professional advisers with which they interact are obliged to comply with the UK anti-money laundering regime, and in most cases are required to observe a higher standard of care in so doing.

The Appendix to this memorandum sets out in tabular form a summary of the application of the UK anti-money laundering regime to persons working in businesses which operate outside the regulated sector.
4. A PRACTICAL EXAMPLE

To appreciate the wide-reaching nature of the UK anti-money laundering legislation, it is helpful to consider a practical example.

Suppose that a company (Company A) operates a manufacturing business; following recent press speculation, the Office of Fair Trading is investigating allegations that Company A, along with manufacturers of similar products, may in the past have colluded with retailers to fix the resale prices for their products – conduct which might amount to an offence under UK competition law. The implications of this scenario under the UK anti-money laundering regime are more extensive than might be expected.

A. Any benefit from the criminal conduct, including any income generated for Company A as a result of any unlawful price-fixing activities, could constitute criminal property under the wide definition in POCA 2002. Furthermore any property which represents such a benefit (whether in whole or in part and whether directly or indirectly) could also be criminal property. If, for example, Company A has assets which have been wholly or partly financed by that income, those assets may also constitute criminal property for the purposes of POCA 2002. Merely possessing or using criminal property is sufficient to constitute a primary money laundering offence.

B. Any transfer of that criminal property (for example if Company A were to seek to sell part of its business) may be money laundering for the purposes of POCA 2002, unless an authorised disclosure is made to SOCA and appropriate consent obtained.

C. If the parent company of Company A takes steps to sell Company A, any individuals working for the parent - and potentially therefore also the parent company itself - may be facilitating the acquisition, use and control of criminal property if they know about or suspect the infringement has occurred (subject to the appropriate consent exception).

D. If a potential purchaser of Company A discovers evidence, in the course of its due diligence, which supports the allegation that Company A has engaged in retail price-fixing in the past (and may therefore be guilty of a criminal offence), the purchaser could potentially be at risk of entering into an arrangement which it knows would facilitate the retention, use or control of criminal property by another person (the purchase price in the hands of the parent company would reflect the value of Company A as inflated by the criminal property – an indirect benefit of Company A’s criminal conduct) (again, subject to the appropriate consent exception). In limited circumstances, Company A could also be at risk of committing the offence of acquiring, using or having possession of criminal property (the benefits in Company A of its criminal activity), although a specific statutory defence is likely to be available for most commercial sales24.

---

24 The offence of acquiring, using or having possession of criminal property is not committed if the acquisition is for “adequate consideration”, as one would expect to be the case where the sale is taking place on arm’s length terms – a specific defence for such acquisitions is set out in section 329(2)(c) of POCA 2002.
E. Any investment banker or accountant working in the regulated sector in the UK who advises the parent on the sale and knows the relevant facts will commit a failure to disclose offence if he does not report the information to his money laundering reporting officer as soon as is practicable, and may also commit the substantive offence of becoming concerned in an arrangement which he knows or suspects facilitates the acquisition, use or control of criminal property (subject to the appropriate consent exception).

F. Any professional legal adviser who knows the relevant facts and acts for any party involved in the transaction could commit a failure to disclose offence if he does not report to SOCA any knowledge or suspicion of money laundering of which he becomes aware in the course of providing legal advice. In many circumstances, a professional legal adviser will seek to rely on the defence of legal professional privilege so as not to be required to disclose to SOCA information received from a client (see section 5 below). When relying on that defence, a professional legal adviser will also need to ensure that he does not commit the substantive offence of becoming concerned in an arrangement which he knows or suspects facilitates the acquisition, use or control of criminal property (subject to the appropriate consent exception); the legal professional privilege defence is not available in respect of this latter substantive offence.

G. Any investment banker, accountant or professional legal adviser reporting the transaction to SOCA will need to take care to avoid alerting any other party involved in the sale and purchase of Company A (including other advisers) of that report so as not to commit a tipping off offence.
5. LEGAL PROFESSIONAL PRIVILEGE

Generally, a firm expects to be able to deal openly with its lawyers and to be able to rely on them to observe strict standards of confidentiality. It is very unusual for a lawyer in the UK to find himself in the position of having to consider whether to report his client to a law enforcement agency, particularly in circumstances where he has been approached for advice in relation to a bona fide commercial transaction. The anti-money laundering legislation therefore represents a very significant development in the relationship between lawyers and their clients. There are circumstances in which a law firm is not obliged to disclose a suspicion that its client may have been involved in the commission of a substantive money laundering offence, but these are more limited than might be expected.

A lawyer must disclose any suspicion of money laundering, save where the information has come to him in "privileged circumstances". Correspondence or discussions with a lawyer will not automatically fall within this exemption – it is only those communications that directly seek or provide legal advice, or that are given in connection with legal proceedings or contemplated legal proceedings (and are not designed to further a criminal purpose) that will be covered. This same exemption applies to other relevant professional advisers, including auditors, accountants and tax advisers, but similarly only to the limited extent that such advisers are carrying out effectively the same functions as lawyers in relation to legal advice.

Whilst it should not be assumed that a lawyer will necessarily be able to tell his client if a disclosure has been made to SOCA, equally it is often possible for a lawyer to seek appropriate consent from SOCA jointly with the client for which he is acting. In almost all cases, however, lawyers will not disclose to any other person the fact that a disclosure has been made, both for reasons of client confidentiality and so as to avoid committing a tipping off offence.

A lawyer may be permitted to tell his client that a disclosure has been made if he does so in connection with the giving of legal advice or, if litigation has started or is reasonably in prospect, in connection with those legal proceedings.
6. CONCLUSION

Given the very wide definition of criminal property for the purposes of the UK’s anti-money laundering legislation, businesses, and individuals working in them, need to recognise that they are at risk of committing quite serious money laundering offences in circumstances which would not, in many cases, give rise to concerns about criminality. This risk arises not only in circumstances where an individual or a business becomes involved with other persons who may be engaged in money laundering, but also in circumstances where the individual or business itself has benefited from conduct which is treated as criminal conduct for the purposes of the UK anti-money laundering regime.

Businesses should also be aware that providers of financial services, professional advice and other regulated sector services will be under a duty to report any suspicion of the commission of a money laundering offence. This duty to report will, in many circumstances, override any duty of confidentiality which such service providers might otherwise owe to their clients.

IMPORTANT NOTE: This memorandum is intended as an introductory guide to the UK’s anti-money laundering regime. It should not be relied upon as a substitute for legal advice.

If you have specific questions relating to anti-money laundering please contact your usual adviser at Slaughter and May or speak directly to Ruth Fox, Ben Kingsley, James Roslington or Sophie Pakenham in Slaughter and May’s Financial Regulation Group on +44 (0) 20 7600 1200.
APPENDIX — SUMMARY OF THE APPLICATION OF LEGISLATIVE PROVISIONS TO
PERSONS WORKING IN BUSINESSES OUTSIDE THE REGULATED SECTOR

The following table sets out the application of the UK’s anti-money laundering regime to persons working in a business which operates outside the regulated sector:

<table>
<thead>
<tr>
<th>Legislative provision</th>
<th>Application to persons working in businesses operating outside the regulated sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money Laundering Regulations</td>
<td>Do not apply</td>
</tr>
<tr>
<td>FSA Handbook</td>
<td>Does not apply</td>
</tr>
<tr>
<td>Proceeds of Crime Act</td>
<td>Primary offences apply</td>
</tr>
<tr>
<td></td>
<td>Failure to disclose offence does not apply*</td>
</tr>
<tr>
<td></td>
<td>Tipping off offence does not apply</td>
</tr>
<tr>
<td></td>
<td>Prejudicing an investigation offence applies</td>
</tr>
<tr>
<td></td>
<td>* Failure to disclose offence does apply to firms which have an MLRO</td>
</tr>
<tr>
<td>Terrorism Act</td>
<td>Primary offences apply</td>
</tr>
<tr>
<td></td>
<td>Section 19 failure to disclose offence applies</td>
</tr>
<tr>
<td></td>
<td>Tipping off offence does not apply</td>
</tr>
<tr>
<td></td>
<td>Prejudicing an investigation offence applies</td>
</tr>
</tbody>
</table>

© Slaughter and May, 2008
CONTACT ADDRESSES

London
One Bunhill Row
London EC1Y 8YY
United Kingdom
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Paris
130 rue du Faubourg Saint-Honoré
75008 Paris
France
T +33 (0)1 44 05 60 00
F +33 (0)1 44 05 60 60

Brussels
Square de Meeûs 40
1000 Brussels
Belgium
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
47th Floor
Jardine House
One Connaught Place
Central
Hong Kong
T +852 2521 0551
F +852 2845 2125

www.slaughterandmay.com