SUPREME COURT
277 MAIN STREET
GIBRALTAR
Tel: (350) 20075608 (Registry) (350) 20075445 (Registrar)
Fax: (350) 20077118

CIRCULAR TO ALL CHAMBERS

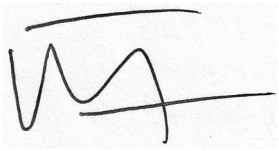
Circ. 14 of 2020 9th October 2020

Issue of Revised Anti-Money Laundering and Combatting Terrorist Financing Guidance Notes

The Guidance Notes revised as at October 2020 have today been issued and are appended hereto. They can also be found on the Gibraltar Court Service website at the AML/CFT page: http://www.gcs.gov.gi/index.php/aml-cft.

The last revision was undertaken and issued in June 2019. The current revision takes account of the EU's Fifth Money Laundering Directive and the various relevant items arising out of the Mutual Evaluation Report on Gibraltar dated 5th December 2019. The revisions have been the subject of previous circulars and publications.

The Revised Guidance Notes are an integral part of the application of the Proceeds of Crimes Act 2015, the Terrorism Act 2018 and related legislation, and, therefore, adherence to them is essential to the continuing supervisory work being undertaken in relation to AML and CFT as well as Targeted Financial Sanctions, and the supervisory response of your firms as providers of legal services.



KARL TONNA
Registrar

Registrar of the Supreme Court

Anti-Money Laundering and Combatting Terrorist Financing Guidance Notes

Legal Professions

1st November 2017
(Updated 9th October 2020)

Table of Contents

Definitions

authorised disclosure	disclosure made to the GFIU in accordance with section 4G POCA, also referred to as a 'suspicious activity report' (SAR)
beneficial owner	see Chapter 4.7
business relationship	a business, professional or commercial relationship which is connected with the professional activities of a relevant financial business and which is expected, at the time when contact is established, to have an element of duration [Section 8 POCA]
confiscation order	Has the meaning given to it under section 35 POCA and also involves the process which the court undergoes to assess whether a person has benefited from criminal conduct and the amount to be recovered even before dealing with that person in respect of any offence committed. The court will consider such a benefit has been obtained if the person has at any time (whether before or after the commencement of POCA) received any payment or other reward in connection with criminal conduct carried on by him or another person
criminal conduct	conduct which– (a) if it occurs in Gibraltar constitutes an offence in Gibraltar; or (b) if it does not occur in Gibraltar would constitute an indictable offence in Gibraltar if it occurred there. [section 182 POCA]
criminal property	property is criminal property if (a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly); and (b) the alleged offender knows or suspects that it constitutes or represents such a benefit. and it is important to note that a person is taken to benefit from criminal conduct if he obtains property or a pecuniary advantage. If a person obtains a pecuniary advantage, he is taken to obtain as a result of or in connection with the conduct a sum of money equal to the value of the pecuniary advantage. [section 182 POCA]
customer due diligence	see Chapter 4
DAML	defence against money laundering – a term used by the GFIU to refer to 'appropriate consent' to carrying out an activity that may result in a person committing a principal money laundering or terrorist financing offence as contained in Part II of POCA and Part II of the TA 2018

GFIU	Gibraltar Financial Intelligence Unit
GFSC	Gibraltar Financial Services Commission
independent legal professional	see chapter 1.1
insolvency practitioner	any person who acts as an insolvency practitioner within the meaning of sections 2 and 476(1) of the Insolvency Act 2011
legal professional privilege	see chapter 6
LSRA	Legal Services Regulatory Authority under section 14 Legal Services Act 2017
Minister	under POCA means Minister responsible for Justice
money laundering	means doing any act which constitutes an offence under section 2 POCA (arrangements) section 3 POCA (acquisition possession or use of criminal property) section 4 POCA (concealing, transferring etc. proceeds of criminal conduct) section 35 TA 2018 (raising funds for terrorism) section 36 TA 2018 (use and possession of money or other property for terrorism) section 37 TA 2018 (arranging funds for terrorism) section 39 TA 2018(arrangement for retention or control of terrorist property) any other act constituting an offence under any enactment that applies in Gibraltar and that offence relates to terrorism or the financing of terrorism, and in the case of an act done outside Gibraltar would constitute such an offence if done in Gibraltar [section 5(9) POCA]
nominated officer	A person nominated within the practice to make disclosures to the GFIU under POCA – also referred to as a 'Money Laundering Reporting Officer' (MLRO).
occasional transaction	A transaction (carried out other than as part of a business relationship) amounting to 15,000 euros or more, whether the transaction is carried out in a single operation or several operations which appear to be linked.
ongoing monitoring	see chapter 4.4
POCA	means the Proceeds of Crime Act 2015 as amended
Politically exposed person or PEP	see chapter 4.9.2
practice	An independent legal practitioner's business, whether that business is a law firm or conducted as a sole practitioner, and applies irrespective of whether that person is a self-employed professional.

privileged circumstances	see chapter 6.5
prohibited act	an act mentioned in section 2(1), 3(1) or 4(1) POCA (also known as the “principal money laundering offences” – see chapter 5.4)
property	means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets [section 183 POCA]
regulated sector	Activities, professions and entities regulated for the purposes of AML/CTF obligations - see chapter 1
Supervisory Authority	the bodies listed in Part I of Schedule 2 of POCA
tax advisor	A practice or sole practitioner who, by way of business, provides advice about the tax affairs of another person, when providing such services
TA 2018	Terrorism Act 2018 as amended
terrorist financing	the use of funds or other assets, or the making available of funds or assets, by any means, directly or indirectly for the purposes of terrorism; or the acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes [section 1ZA POCA]
terrorist property	Money or other property which is likely to be used for the purposes of terrorism, the proceeds of the commission of acts of terrorism and the proceeds of acts carried out for the purposes of terrorism [section 5(1) TA 2018]
working day	is a day other than a Saturday, a Sunday, or a day which is a bank or public holiday pursuant to an order made under the Banking and Financial Dealings Act or the Interpretation and General Clauses Act [section 4A(7) POCA]

Chapter 1 Introduction

1.1 Who should read these Guidance Notes?

All notaries, lawyers and other staff in a law firm who are involved in anti-money laundering and terrorist financing compliance. For the purpose of these Guidance Notes, any reference to the term lawyers will be deemed to include barristers, solicitors, legal executives and any other person acting or authorised to act in law or acting under the supervision of a person legally authorised to act. Similarly, any reference to independent legal professional means a firm or a sole practitioner who by way of business provides legal or notarial services to other persons. It does not include legal professionals employed by a public authority or working in-house.

1.2 What is the issue?

Lawyers and notaries are key professionals in the business and financial world, facilitating vital transactions that underpin the Gibraltar economy. As such, they have a significant role to play in ensuring their services are not abused to further a criminal purpose. As professionals, lawyers and notaries must act with integrity and uphold the law, and they must not engage in criminal activity.

Money laundering and terrorist financing are serious threats to society, losing revenue and endangering life, and fuelling other criminal activity.

These Guidance Notes aim to assist lawyers and notaries in Gibraltar to meet their obligations under the Gibraltar anti-money laundering and counter-terrorist financing (AML/CTF) regime.

1.3 Definition of money laundering

Money laundering is generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come from a legitimate source. Under the Proceeds of Crime Act 2015 (“POCA”), the definition contained in section 5(9) POCA is broader and more subtle, and means doing any act which constitutes certain types of offences found in both POCA and the Terrorism Act 2018 (“TA”), as well as any act which constitutes an offence under any other applicable enactment in Gibraltar that relates to terrorism or the financing of terrorism, even if the act is done outside Gibraltar. It should be noted that the term ‘money laundering’ consists of both the traditional use of the word as well as ‘terrorist financing’ throughout Part III of POCA.

Money laundering can arise from small profits and savings from relatively minor crimes, such as regulatory breaches, minor tax evasion or benefit fraud. A deliberate attempt to obscure the ownership of illegitimate funds is not necessary.

There are three acknowledged phases to money laundering: placement, layering and integration. However, the broader definition of money laundering offences in POCA includes even passive possession of criminal property as money laundering.

1.3.1 Placement

Cash generated from crime is placed in the financial system. This is the point when proceeds of crime are most apparent and at risk of detection. Because banks and financial institutions have developed AML procedures, criminals look for other ways of placing cash within the financial system. You can be targeted because a lawyer's firm commonly deals with client money. Notaries may also deal with client money.

1.3.2 Layering

Once proceeds of crime are in the financial system, layering obscures their origins by passing the money through complex transactions. These often involve different entities like companies and trusts and can take place in multiple jurisdictions. You may be targeted at this stage and detection can be difficult.

1.3.3 Integration

Once the origin of the funds has been obscured, the criminal is able to make the funds reappear as legitimate funds or assets. They will invest funds in legitimate businesses or other forms of investment, often using you to buy a property, set up a trust, acquire a company, or even settle litigation, among other activities. This is the most difficult stage of money laundering to detect.

1.4 Legal framework and other requirements

1.4.1 Financial Action Task Force (FATF)

This was created in 1989 by the G7 Paris summit, building on UN treaties on trafficking of illicit substances in 1988 and confiscating the proceeds of crime in 1990.

In 1990, FATF released their 40 recommendations for fighting money laundering. Between October 2001 and October 2004, it released nine further special recommendations to prevent terrorist funding. In February 2012 these recommendations were substantially revised and through a continual process of revisions and updates continue to be elaborated to keep up to date with current threats and vulnerabilities.

1.4.2 European Union Directives

1991 – First Money Laundering Directive

The European Commission issued this to comply with the FATF recommendations. It applied to financial institutions, and required member states to make money laundering a criminal offence. It was incorporated into Gibraltar law via the Crime (Money Laundering and Proceeds) Act 2007 ("CMLPA" – originally called the Criminal Justice Act 1995) and the Drug Trafficking Offences Act 1995.

2001 – Second Money Laundering Directive

This incorporated the amendments to the FATF recommendations. It extended anti-money laundering obligations to a defined set of activities provided by a number of service professionals, such as independent legal professionals, accountants, auditors, tax advisors and real estate agents. The legislation current at the time was amended to incorporate these changes in the Criminal Justice (Amendment) Act 2004.

2005 – Third Money Laundering Directive (3MLD)

Gibraltar was compliant with 3MLD primarily through the transposition in POCA as well as regulatory and supervisory processes that are applicable to relevant financial business therein. Lawyers were, since 2005, required to comply with the provisions of 3MLD.

2017 – Fourth Money Laundering Directive (4MLD)

In order to keep pace with the revised FATF Recommendations as well as to address EU specific risks, 3MLD has been replaced with 4MLD[1]. This Directive is more prescriptive in its

[1] DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

approach as to the national transposition requirements but broadly follows the FATF recommendations. In some cases, however, it has adopted a more granular approach to specific requirements. One major change brought about by 4MLD is a new requirement for EU Member States to maintain a central beneficial ownership register (Articles 30 and 31).

4MLD was transposed into local legislation in stages, with full transposition achieved by 28th June 2017 Gibraltar has not only made substantial amendments to POCA, but also other legislative texts in order to fully transpose 4MLD. The below is a list of key pieces of legislation that have recently transposed 4MLD:

- Proceeds of Crime Act 2015 (Amendment) Act 2017
- Proceeds of Crime Act 2015 (Amendment) Regulations 2017
- Register of Ultimate Beneficial Owners Regulations 2017

It is important to also note that, in exercise of the powers conferred upon him by regulation 5 of the Register of Ultimate Beneficial Owners Regulations 2017, by Legal Notice 121 of 2017, the Minister has appointed the Finance Centre Director as the Registrar of Ultimate Beneficial Owners under those Regulations.

1.4.3 Terrorism Act 2018 (TA)

The TA was introduced to deal with Council Framework Decision 2002/475/JHA on the Combatting of Terrorism.

The TA 2018establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. It is modelled on the Terrorism Act 2000 of the UK, which establishes a list in the Schedule to that Act of proscribed organisations whom are involved in terrorism.

Read about these provisions in Chapter 7

Application

The TA 2018 applies to all persons. There is a defence to most of the offences contained in TA 2018 if a person discloses to the Gibraltar Financial Intelligence Unit ("GFIU") their suspicion that money or other property is terrorist property and the information on which their suspicion or belief is based, and the GFIU gives express consent for that person to act in contravention of the TA 2018. There are exceptions[2] in limited circumstances for certain professionals. There are offences for receiving client money or property that intends to be used, or you have reasonable cause to suspect that it may be used, for the purposes of terrorism.

1.4.4 Terrorist Asset-Freezing Regulations 2011 (TAFR)

These regulations impose restrictive measures directed against certain persons and entities with a view to combatting terrorism and implements UN Security Council Resolutions.

1.4.5 Counter Terrorism Act 2010 (CTA)

This Act imposes countermeasures against countries, territories, governments, individuals and corporate persons in connection with terrorist financing, money laundering and proliferation of weapons of mass destruction.

[2] Section 9A of the TA.

1.4.6 Proceeds of Crime Act 2015 ("POCA")

The CMLPA was repealed and replaced by POCA in 2015. POCA establishes a number of money laundering offences including:

- principal money laundering offences
- offences of failing to report suspected money laundering
- offences of tipping-off about a money laundering disclosure, tipping-off about a money laundering investigation, tipping-off, and prejudicing money laundering investigations.

Application

POCA applies to all persons, although certain failure to report offences only apply to persons who are engaged in activities in a relevant financial business.

It also sets out administrative requirements for the anti-money laundering regime within the relevant financial businesses and outlines the scope of customer due diligence. The aim is to limit the use of professional services for money laundering by requiring professionals to know their clients and monitor the use of their services by clients.

Under section 9 POCA, key activities that would cause you to operate in a relevant financial business which may be relevant to you are the provision by way of business, in one of the following ways:

(i) notaries and other independent legal professionals, when they participate whether–

  (i) by assisting in the planning or execution of transactions for their client concerning the;

    (A) buying and selling of real property or business entities;

    (B) managing of client money, securities or other assets;

    (C) opening or management of bank, savings or securities accounts;

    (D) organisations of contributions necessary for the creation, operation or management of companies;

    (E) creation, operation or management of trusts, companies, foundations, or similar structures; or

  (ii) by acting on behalf of and for their client in any financial or real estate transaction;

You will be participating in a transaction by assisting in the planning or execution of the transaction or otherwise acting for or on behalf of a client in the transaction.

Part 3 of POCA aims to limit the use of professional services for money laundering by requiring professionals to know their clients and monitor the use of their services by clients.

Section 9 POCA states that POCA also applies to persons acting in the course of businesses carried on in Gibraltar in the following areas:

- electronic money issuer or deposit-taking business
- the Savings Bank or the Gibraltar International Bank,
- regulated activities carried on by a European institution
- investment business
- financial and credit institutions
- insurance business (but not general insurance intermediaries)
- auditors, insolvency practitioners, external accountants and tax advisers
- real estate agents
- trust or company service providers
- high value dealers (cash payments in amounts of EUR10,000 or more)

- casinos / gambling services
- currency exchange offices / bureaux de change
- money transmission / remittance offices
- collective investment schemes

Activities covered by POCA

In terms of the key activities covered, note that:

- managing client money is narrower than handling it; and
- opening or managing a bank account (including savings or securities accounts) is wider than simply opening a lawyers' or notaries client account. It would be likely to cover them acting as a trustee, attorney or a receiver

Activities not covered by POCA

The following would not generally be viewed as participation in financial transactions:

- payment on account of costs to a lawyer or to a notary or payment of a bill
- provision of legal advice
- participation in litigation or a form of alternative dispute resolution
- will-writing, although you should consider whether any accompanying taxation advice is covered.

You must also consider the full range of related services, such as tax planning and tax compliance work.

If you are a notary public or act as a commissioner for oaths you should consider whether the type of work you carry out whether your activities carry a risk of money laundering. For example, POCA does not apply to work undertaken by a notary as a public certifying officer where he or she has no substantive role in the underlying transaction. As such, it does not apply to many aspects of a notary's practice including, for example, the taking of affidavits and declarations, protests, translating, certifying the execution of documents and authentication work in general. Although the provisions of POCA will not apply to work of this nature, notaries are still subject to their own codes of practice.

You will also need to consider whether your firm undertakes activities falling within the definition of relevant financial business under POCA and whether a Supervisory Authority has also issued Guidance Notes on that sector which are applicable to the carrying out of those duties.

If you are an independent legal professional within the regulated sector and you also fall within another category, such as work regulated by the Gibraltar Financial Services Commission ("GFSC"), this may affect your supervision under applicable legislation. You should contact the GFSC for advice on any supervisory arrangements that they may have in place with other Supervisory Authorities.

Chapters 5, 6, and 8 of these Guidance Notes provide more details on your obligations under POCA.

1.5 Status of these Guidance Notes

1.5.1 Legal Basis for the Notes

Section 33(2) of POCA provides, inter alia, as follows:

"In deciding whether a person has committed an offence under subsection (1), the court must consider whether he followed any relevant guidance which was at the time issued by a Supervisory Authority or any other appropriate body." The Notes are drawn up considering the above provisions.

The Notes are, therefore, intended to interpret the requirements of POCA in a practical manner. They are intended to illustrate good industry practice. The key question, however, is whether a relevant financial business is obliged to comply with the provisions of the Notes.

The word "must" in section 33(2) of POCA imports an obligation on the Courts to "consider" the Notes in determining whether a person has complied with POCA.

For this reason, the provisions and the structure of POCA must be taken as a whole. Part III creates an obligation on relevant financial businesses to establish and maintain certain standards and procedures to combat money laundering and terrorist financing – the Act is not, however, prescriptive on how these requirements should be fulfilled. It is suggested that it was clearly intended that this would be left to industry practice as embodied in the Notes and that a judge, in determining whether a breach had been committed, would be obliged to consider such guidance issued by the regulatory authorities.

By way of summary: -

(a) the Notes are written in such a way that compliance with its terms is obligatory;

(b) if there is non-compliance with the Notes, a judge must consider such non-compliance when determining whether a person is in breach of the provisions of section POCA;

(c) the result of the combination of (a) and (b) immediately above is that a judge, save in an exceptional case, must hold that a person who does not comply with the terms of the Notes is in breach of the provisions of POCA.

It follows that, if a person does not adhere to the provisions of the Notes, such person would be applying the standards of practice falling below best market practice and would not be held to have taken all reasonable steps and exercised all due diligence.

1.6 Terminology in these Guidance Notes

Must

A specific requirement in legislation or of a principle, rule, outcome or other mandatory provision in the codes of conduct applicable to lawyers ("the Applicable Codes").

You must comply, unless there are specific exemptions or defences provided for in relevant legislation.

Note: As the regulatory environment in legal services is presently in transition there are references in these Guidance Notes to the handbooks issued by the English Solicitors Regulation Authority and Bar Standard Board. These documents will cease to have any applicability following the full commencement of the Legal Services Act 2017 but are mentioned herein insofar as they have current application.

For the purpose of these Guidance Notes, it will be presumed that any reference to the SRA Handbook will also be taken to include a reference to the BSB Handbook. Further any references to a particular Principle found in the SRA Handbook will be taken to include a reference to an equivalent principle in the BSB Handbook, where such equivalence exists.

As indicated above it is the Code of Conduct to be issued under the Legal Services Act will replace previous Applicable Codes.

Should

- Outside of a regulatory context, good practice for most situations in the Registrar's view.
- In the case of the SRA Handbook, an indicative behaviour or other non-mandatory provision (such as may be set out in notes or guidance).

These may not be the only means of complying with legislative or regulatory requirements and there may be situations where the suggested route is not the best possible route to meet the needs of your client. However, if you do not follow the suggested route, you should be able to justify to the Supervisory Authority why the alternative approach you have taken is appropriate, either for your practice, or in the particular retainer.

May

A non-exhaustive list of options for meeting your obligations or running your practice. Which option you choose is determined by the profile of the individual practice, client or retainer. You may be required to justify why this was an appropriate option to oversight bodies.

Chapter 2 The Risk-Based Approach

2.1 General Comments

The possibility of being used to assist with money laundering and terrorist financing poses many risks for your firm, including:

- criminal and disciplinary sanctions for firms, individual lawyers and notaries
- civil action against the firm as a whole and individual partners
- damage to reputation leading to a loss of business

These risks must be identified, assessed and mitigated, just as you do for all business risks facing your firm. If you know your client well and understand your instructions thoroughly, you will be better placed to assess risks and spot suspicious activities. Applying the risk-based approach will vary between firms. While you can, and should, start from the premise that most of your clients are not launderers or terrorist financers, you must assess the risk level particular to your firm and implement reasonable and considered controls to minimise those risks.

No matter how thorough your risk assessment or how appropriate your controls, some criminals may still succeed in exploiting you for criminal purposes. But an effective, risk-based approach and documented, risk-based judgements on individual clients and retainers will enable your firm to justify your position on managing the risk to law enforcement, courts and Supervisory Authorities.

The risk-based approach means that you focus your resources on the areas of greatest risk. The resulting benefits of this approach include:

- more efficient and effective use of resources proportionate to the risks faced
- minimising compliance costs and burdens on clients
- greater flexibility to respond to emerging risks as laundering and terrorist financing methods change

2.2 Application

POCA requires a risk-based approach for compliance with customer due diligence obligations.

This approach does not apply to reporting suspicious activity, because POCA and the TA 2018 lay down specific legal requirements not to engage in certain activities and to make reports of suspicious activities once a suspicion is held. [See chapters 5 and 7] The risk-based approach still applies to ongoing monitoring of clients and retainers which enables you to identify suspicions.

2.3 Assessing your firm's risk profile

This depends on your firm's size, type of clients, and the practice areas it engages in.

You should consider the following factors:

2.3.1 Client demographic

Your client demographic can affect the risk of money laundering or terrorist financing. Factors which may vary the risk level include whether you:

- have a high turnover of clients or a stable existing client base
- act for politically exposed persons (PEPs)
- act for clients without meeting them
- provide services in respect of locations with high levels of acquisitive crime or for clients who have convictions for acquisitive crimes, which increases the likelihood the client may possess criminal property
- act for clients affiliated to countries with high levels of corruption or where terrorist organisations operate
- act for entities that have a complex ownership structure
- are easily able to obtain details of beneficial owners of your client or not

2.3.2 Services and areas of law

Some services and areas of law could provide opportunities to facilitate money laundering or terrorist financing. For example:

- complicated financial or property transactions
- providing assistance in setting up trusts or company structures, which could be used to obscure ownership of property
- payments that are made to or received from third parties
- payments made by cash
- transactions with a cross-border element

Simply because a client or a retainer falls within a risk category does not mean that money laundering or terrorist financing is occurring. You need to ensure your internal controls are designed to address the identified risks and take appropriate steps to minimise and deal with these risks.

Chapter 11 provides more information on warning signs to be alert to when assessing risk.

2.4 Assessing individual risk

Determining the risks posed by a specific client or retainer will then assist in applying internal controls in a proportionate and effective manner.

Under section 11(5) POCA you must at least, take into account the following list of risk variables When determining to what extent to apply customer due diligence measures:

- the purpose of an account or relationship
- the level of assets to be deposited by a customer or the size of transactions undertaken
- the regularity or duration of the business relationship

You may consider whether:

- your client is within a high-risk category
- you can be easily satisfied that the customer due diligence (“CDD”) material for your client is reliable and allows you to identify the client and verify that identity
- you can be satisfied you understand their control and ownership structure
- the retainer involves an area of law at higher risk of laundering or terrorist financing
- your client wants you to handle funds without an underlying transaction, contrary to the Solicitors' Accounts Rules (“SAccR”)

- there are any aspects of the particular retainer which would increase or decrease the risks

This assessment helps you adjust your internal controls to the appropriate level of risk presented by the individual client or the particular retainer. Different aspects of your CDD controls will meet the different risks posed:

- If you are satisfied you have verified the client's identity, but the retainer is high risk, you may require fee earners to monitor the transaction more closely, rather than seek further verification of identity.
- If you have concerns about verifying a client's identity, but the retainer is low risk, you may expend greater resources on verification and monitor the transaction in the normal way.

Risk assessment is an ongoing process both for the firm generally and for each client, business relationship and retainer. In a lawyer's or notarial practice, it is the overall information held by the firm gathered while acting for the client that will inform the risk assessment process, rather than sophisticated computer data analysis systems. The more you know your client and understand your instructions, the better placed you will be to assess risks and spot suspicious activities.

Section 25A of POCA imposes additional risk assessment obligations on relevant financial businesses; you must take appropriate steps to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors including those relating to

- customers,
- countries or geographic areas
- products
- services, transactions
- delivery channels,

In addition, you must take account of any information that is made available by the GFIU pursuant to the National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing Regulations 2016.

Although already a requirement under the AMLGNs, POCA now puts into statute that it is the responsibility of a director, senior manager or partner to ensure the firm’s compliance with Parts II and III of POCA.

In accordance with section 26A POCA, a firm’s policies, controls and procedures must not be implemented without the prior approval of senior management; this category of individual(s) is defined in section 7 POCA as follows:

“senior management” means an officer or employee with sufficient knowledge of the institution’s money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

Chapter 3 Systems, Policies and Procedures

3.1 General Comments

Develop systems to meet your obligations and risk profile in a risk-based and proportionate manner. Policies and procedures supporting these systems mean that staff apply the systems consistently and firms can demonstrate to oversight bodies that processes facilitating compliance are in place.

3.2 Application

Part 3 of POCA requires a relevant financial business to have certain systems in place. Failing to have those systems in place is an offence, punishable by a fine or up to two years' imprisonment, or both. You must demonstrate your compliance to the Supervisory Authority designated under POCA, as supervisor under this legislation.

The Sanctions Act 2015 also imposes new requirements on relevant financial businesses with regards to checking of persons or other entities subjected to sanctions.

If you are outside the regulated sector, you should still consider how these systems can assist you to comply with your obligations to report suspicious transactions in accordance with POCA and the TA 2018.

3.3 The Appropriate Person or the Money Laundering Reporting Officer

3.3.1 Why have an appropriate person?

Section 26(2) (d) (i) POCA requires that all firms within the regulated sector must have an “appropriate person” (better known as the Money Laundering Reporting Officer or MLRO) to receive disclosures under section 28 POCA, and to make disclosures to the GFIU.

Section 26(3) POCA provides that there is no requirement to have an appropriate person in a relevant financial business if you are an individual who operates in a relevant financial business but does not employ any people or act in association with anyone else.

Firms who do not provide services as a relevant financial business should consider appointing an appropriate person, even though it is not required, because POCA and the TA 2018 still apply.

3.3.2 Who should be the appropriate person?

Your appropriate person should be of sufficient seniority to make decisions on reporting which can impact your firm's business relations with your clients and your exposure to criminal, civil, regulatory and disciplinary sanctions. They should also be in a position of sufficient responsibility to enable them to have access to all of your firm's client files and business information to enable them to make the required decisions on the basis of all information held by the firm. Section 26(1) (f) POCA requires that (where appropriate with regard to the size and nature of the business) firms should have appropriate controls and procedures that allow for compliance management and the allocation of overall responsibility for the establishment and maintenance of effective systems of control to a compliance officer at management level (being a director or senior manager).

3.3.3 Role of the appropriate person

Your appropriate person is responsible for ensuring that, when appropriate, the information or other matter leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the relevant authority. The decision to report, or not to report, must not be subject to the consent of anyone else. Your appropriate person will also liaise with the GFIU or law enforcement on the issue of whether to proceed with a transaction or what information may be disclosed to clients or third parties.

The size and nature of some firms may lead to the appropriate person delegating certain duties regarding the firm's AML/CTF obligations. In some large firms, one or more permanent deputies of suitable seniority may be appointed. All firms will need to consider arrangements for temporary cover when the appropriate person is absent.

3.4 Risk assessment

You can extend your existing risk management systems to address AML and CTF risks. The detail and sophistication of these systems will depend on your firm's size and the complexity of the business it undertakes. Ways of incorporating your risk assessment of clients, business relationships and transactions into the overall risk assessment will be governed by the size of your firm and how regularly compliance staff and senior management are involved in day-to-day activities.

Issues which may be covered in a risk assessment system include:

- the firm's current risk profile
- how AML/CTF risks will be assessed, and processes for re-assessment and
- updating of the firm's risk profile
- internal controls to be implemented to mitigate the risks
- which firm personnel have authority to make risk-based decisions on compliance
- on individual files
- how compliance will be monitored and effectiveness of internal controls will be reviewed

3.5 Internal controls and monitoring compliance

The level of internal controls and extent to which monitoring needs to take place will be affected by:

- your firm's size
- the nature, scale and complexity of its practice
- its overall risk profile

Issues which may be covered in an internal controls system include:

- the level of personnel permitted to exercise discretion on the risk-based application of POCA, and under what circumstances
- CDD requirements to be met for simplified, standard and enhanced due diligence
- when outsourcing of CDD obligations or reliance will be permitted, and on what conditions
- how you will restrict work being conducted on a file where CDD has not been completed
- the circumstances in which delayed CDD is permitted
- when cash payments will be accepted
- when payments will be accepted from or made to third parties
- the manner in which disclosures are to be made to the nominated officer
- employee screening
- independent audit

As a new requirement introduced in 2017, employee screening is required under section 26(1) (g) POCA to identify if criminals are involved with a relevant financial business. This applies at all levels of employment and not at senior management level.

It is up to the Supervisory Authorities to prevent persons convicted of a relevant offence or their associates from holding a management function in, or being a beneficial owner of, those businesses. (section 30(3) POCA)

In establishing whether a person is fit and proper to hold a management function or be a beneficial owner or shareholder or controller of a relevant financial business, the Supervisory Authorities are now required to conduct criminal checks and make enquiries of the Commissioner of Police under the Exchange of Criminal Records Regulations 2014 (section 30C POCA).

Monitoring compliance will assist you to assess whether the policies and procedures you have implemented are effective in forestalling money laundering and terrorist financing opportunities within your firm. Issues which may be covered in a compliance system include:

- procedures to be undertaken to monitor compliance, which may involve:
- random file audits
- file checklists to be completed before opening or closing a file
- a nominated officer's log of situations brought to their attention, queries from staff and reports made
- reports to be provided from the nominated officer to senior management on compliance
- how to rectify lack of compliance, when identified
- how lessons learnt will be communicated back to staff and fed back into the risk profile of the firm

In addition under section 26(1A) POCA relevant financial businesses are now, where appropriate and having regard to the size and nature of the business, required to undertake an independent audit function which tests its policies, controls and procedures..

Under section 28 POCA, larger firms which form part of a group should ensure the group has in place an adequate reporting procedure for the purposes of receiving disclosures about knowledge or suspicions of money laundering or terrorist financing that may be taking place in regards to activities related to the group.

3.6 Customer due diligence

You are required to have a system outlining the CDD measures to be applied to specific clients. You should consider recording your firm's risk tolerances to be able to demonstrate to your supervisor that your CDD measures are appropriate.

Your CDD system may include:

- when CDD is to be undertaken
- information to be recorded on client identity
- information to be obtained to verify identity, either specifically or providing a range of options with a clear statement of who can exercise their discretion on the level of verification to be undertaken in any particular case
- when simplified due diligence may occur
- what steps need to be taken for enhanced due diligence
- what steps need to be taken to ascertain whether your client is a PEP
- when CDD needs to occur and under what circumstances delayed CDD is permitted
- how to conduct CDD on existing clients
- what ongoing monitoring is required

For suggested methods on how to conduct CDD see Chapter 4 of these Guidance Notes.

3.7 Disclosures

Firms, but not sole practitioners who have no other staff, need to have a system clearly setting out the requirements for making a disclosure under POCA and the TA 2018. These may include:

- the circumstances in which a disclosure is likely to be required
- how and when information is to be provided to the nominated officer or their deputies
- resources which can be used to resolve difficult issues around making a disclosure
- how and when a disclosure is to be made to the GFIU
- how to manage a client when a disclosure is made while waiting for consent
- the need to be alert to tipping-off issues

For details on when a disclosure needs to be made see chapters 5, 6 and 7 of these Guidance Notes. For details on how to make a disclosure see chapter 8 of these Guidance Notes.

3.8 Record keeping

Various records must be kept to comply with POCA and defend any allegations against the firm in relation to money laundering and failure to report offences. A firm's records system must outline what records are to be kept, the form in which they should be kept and how long they should be kept.

Section 25 POCA requires that firms keep records of CDD material and supporting evidence and records in respect of the relevant business relationship or occasional transaction. Adapt your standard archiving procedures for these requirements.

3.8.1 CDD material

You may keep either a copy of verification material, or references to it. Keep it for five years after the business relationship ends or the occasional transaction is completed. Consider holding CDD material separately from the client file for each retainer, as it may be needed by different practice groups in your firm.

Depending on the size and sophistication of your firm's record storage procedures you may wish to:

- scan the verification material and hold it electronically
- take photocopies of CDD material and hold it in hard copy with a statement that the original has been seen
- accept certified copies of CDD material and hold them in hard copy
- keep electronic copies or hard copies of the results of any electronic verification checks
- record reference details of the CDD material sighted

The option of merely recording reference details may be particularly useful when taking instructions from clients at their home or other locations away from your office. The types of details it would be useful to record include:

- any reference numbers on documents or letters
- any relevant dates, such as issue, expiry or writing
- details of the issuer or writer
- all identity details recorded on the document

Where you are relied upon by another person under section 23 POCA for the completion of CDD measures, you must keep the relevant documents for five years from the date on which you were relied upon.

3.8.2 Risk assessment notes

You should consider keeping records of decisions on risk assessment processes of what CDD was undertaken. This does not need to be in significant detail, but merely a note on the CDD file stating the risk level you attributed to a file and why you considered you had sufficient CDD information. For example:

> *'This is a low risk client with no beneficial owners providing medium risk instructions.*
>
> *Standard CDD material was obtained and medium level ongoing monitoring is to occur.'*

Such an approach may assist firms to demonstrate they have applied a risk-based approach in a reasonable and proportionate manner. Notes taken at the time are better than justifications provided later.

Firms may choose standard categories of comment to apply to notes.

3.8.3 Supporting evidence and records

You must keep all original documents or copies admissible in court proceedings.

Records of a particular transaction, either as an occasional transaction or within a business relationship, must be kept for five years after the date the transaction is completed.

All other documents supporting records must be kept for five years after the completion of the business relationship.

3.8.4 Suspicions and disclosures

It is recommended that you keep comprehensive records of suspicions and disclosures because disclosure of a suspicious activity is a defence to criminal proceedings. Such records may include notes of:

- ongoing monitoring undertaken and concerns raised by fee earners and staff
- discussions with the nominated officer regarding concerns
- advice sought and received regarding concerns
- why the concerns did not amount to a suspicion and a disclosure was not made
- copies of any disclosures made
- conversations with the GFIU, law enforcement, insurers, Supervisory Authorities etc. regarding disclosures made
- decisions not to make a report to the GFIU which may be important for the nominated officer to justify his position to law enforcement

You should ensure records are not inappropriately disclosed to the client or third parties to avoid offences of tipping-off and prejudicing an investigation, and to maintain a good relationship with your clients. This may be achieved by maintaining a separate file, either for the client or for the practice area.

3.8.5 Data protection

The Data Protection Act 2004 (“DPA”) applies to you and the GFIU. It allows clients or others to make subject access requests for data held by them. Such requests could cover any disclosures made.

Section 19(2) DPA states you need not provide personal data where disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

If you decide the Section 19(2) DPA exception applies, document steps taken to assess this, to respond to any enquiries by relevant statutory bodies.

Section 34A POCA makes it clear that data subjects' rights are paramount, and only subject to such limitations as may be lawfully prescribed under the DPA; therefore, nothing in POCA affects those rights unless there is a specific provision of POCA stating otherwise. Under POCA the specific provision is section 34A (2) which states that personal data may only be processed by relevant financial businesses on the basis of Part II and Part III POCA only for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 of the 4MLD and shall not be further processed in a way that is incompatible with those purposes (for example, for commercial purposes).

Relevant financial businesses must provide new clients with the information required pursuant to section 10 of the Data Protection Act 2004 before establishing a business relationship or carrying out an occasional transaction and must, in particular, include a general notice concerning the legal obligations to process personal data for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 of the 4MLD.

The information required under section 10 DPA is

(a) the identity of the data controller;
(b) if he has nominated a representative for the purposes of this Act, the identity of the representative;
(c) the purpose or purposes for which the data are intended to be processed; and
(d) any other information which is necessary, having regard to specific circumstances in which the data are or are to be processed, to enable processing in respect of the data to be fair to the data subject such as information–
    (i) as to the recipients or categories of recipients of the data;
    (ii) as to whether replies to questions asked for the purpose of the collection of the data are obligatory;
    (iii) as to the possible consequences of failure to give such replies; and
    (iv) as to the existence of the right of access to and the right to rectify the data concerning him.

And if the data controller (i.e. your firm) has not obtained data directly from the data subject, then in addition to (a) – (d) above, data subjects must be provided with (i) the categories of data concerned; and (ii) the name of the original data controller.

See also chapter 8.5 for further rights of data subjects under DPA and in particular their right under section 14 DPA.

3.8.6 Destruction of records

Under section 25(10) POCA, you are required to delete personal data upon expiry of the 5-year periods mentioned in section 25 POCA unless retention is required by another enactment or where the Minister by Order provides for the retention of records specified in such Order.

3.8.7 Record keeping and legal proceedings

Under section 25ZA POCA, you are allowed to retain (note the section says “may” and not “must”) information and documents which are necessary evidence of the customer’s identity where this information is related to legal proceedings which commenced prior to 25 June 2015, but only until 25 June 2020, after which such information must be destroyed unless retention is required by another enactment or where the Minister by Order provides for the retention of records specified in such Order.

3.9 Communication and training

Your staff members are the most effective defence against launderers and terrorist financers who would seek to abuse the services provided by your firm.

Section 26 POCA requires that you communicate your AML/CTF obligations to your staff, while section 27 POCA requires that you give staff appropriate training on their legal obligations and information on how to recognise and deal with money laundering and terrorist financing risks. Section 27 POCA was recently expanded following transposition of 4MLD to include making staff aware of relevant data protection requirements

3.9.1 Criminal sanctions and defences

Receiving insufficient training is a defence for individual staff members who fail to report a suspicion of money laundering, provided they did not know or suspect money laundering. However, it is not a defence to terrorist funding charges, and leaves your firm vulnerable to sanctions under POCA for failing to properly train your staff.

3.9.2 Who should be trained?

When setting up a training and communication system you should consider:

- which staff require training
- what form the training will take
- how often training should take place
- how staff will be kept up-to-date with emerging risk factors for the firm

Assessments of who should receive training should include who deals with clients in areas of practice within the regulated sector, handles funds or otherwise assists with compliance. Consider fee earners, reception staff, administration staff and finance staff, because they will each be differently involved in compliance and so have different training requirements.

Training can take many forms and may include:

- face-to-face training seminars
- completion of online training sessions
- attendance at AML/CTF conferences
- participation in dedicated AML/CTF forums
- review of publications on current AML/CTF issues
- firm or practice group meetings for discussion of AML/CTF issues and risk factors

Providing an AML/CTF policy manual is useful to raise staff awareness and can be a continual reference source between training sessions.

3.9.3 How often?

You must give your employees relevant training at regular and appropriate intervals. In determining whether your training programme meets this requirement, you should have regard to the firm's risk profile and the level of involvement certain staff have in ensuring compliance.

You should consider retaining evidence of your assessment of training needs and steps taken to meet such needs.

You should also consider:

- criminal sanctions and reputational risks of non-compliance
- developments in the common law
- changing criminal methodologies

Some type of training for all relevant staff every two years is preferable.

3.9.4 Communicating with your clients

While not specifically required by POCA/TA 2018, it useful for you to tell your client about your AML/CTF obligations. Clients are then generally more willing to provide required information when they see it as a standard requirement.

You may wish to advise your client of the following issues:

- the requirement to conduct CDD to comply with POCA
- whether any electronic verification is to be undertaken during the CDD process
- the requirement to report suspicious transactions

Consider the manner and timing of your communications, for example whether the information will be provided in the standard client care letter or otherwise.

As always, be aware that one thing is to tell your client about your obligations, but you should always ensure you are not doing anything that will constitute tipping-off under POCA.

Chapter 4 Customer Due Diligence

4.1 General Comments

Customer due diligence ("CDD") is required by POCA because you can better identify suspicious transactions if you know your customer and understand the reasoning behind the instructions they give you.

4.2 Application

You must conduct CDD on those clients who retain you for services regulated under POCA (see Part III of POCA). See also chapters 2 and 3 of these Guidance Notes.

4.3 CDD in general

4.3.1 When is CDD required?

Section 11 POCA requires that you conduct CDD when:

- establishing a business relationship
- carrying out an occasional transaction
- you suspect money laundering or terrorist financing
- you doubt the veracity or adequacy of documents, data or information previously obtained for the purpose of CDD

You must also apply CDD measures on a risk-sensitive basis, when-

- the relevant circumstances of a customer change
- a legal duty arises pursuant to POCA (or its subsidiary regulations) to contact the customer for the purpose of reviewing any information relating to the beneficial owner or beneficial owners
- pursuant to Parts I, IA and IB of the Income Tax Act
- pursuant to the Tax (Mutual Administrative Assistance) Act 2014

You must also apply CDD measures to a trust, corporate or legal entity which is subject to the registration of beneficial ownership information pursuant to Articles 30 or 31 of the Money Laundering Directive, the relevant financial business shall collect proof of registration or an excerpt of the relevant register.

In Gibraltar, this would be the Gibraltar Ultimate Beneficial Ownership Register https://ubosearch.egov.gi (registration required).The distinction between occasional transactions and long-lasting business relationships is relevant to the timing of CDD and the storage of records.

Where an occasional transaction is likely to increase in value or develop into a business relationship, consider conducting CDD early in the retainer to avoid delays later. As relationships change, firms must ensure they are compliant with the relevant standard.

There is no obligation to conduct CDD in accordance with POCA for retainers involving non-relevant financial businesses.

4.3.1.1 Existing business relationships before 1st February 2018

You must apply CDD measures at appropriate times to existing clients on a risk- sensitive basis. You are not required to apply CDD measures to all existing clients immediately after 1st February 2018. Where you have verified a client's identity to a previously applicable standard then, unless circumstances indicate the contrary, the risk is likely to be low. If you

have existing high-risk clients that you have previously identified, you may consider applying the new CDD standard sooner than for low risk clients.

4.3.2 What is CDD?

Section 10 POCA says that CDD comprises:

(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant financial business is satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and

(c) obtaining information on the purpose and intended nature of the business relationship

4.3.2.1 Identification and verification

Identification of a client or a beneficial owner is simply being told or coming to know a client's identifying details, such as their name and address.

Verification is obtaining some evidence which supports this claim of identity.

4.3.2.2 A risk-based approach

Section 11(3) POCA provides that you must:

(a) determine the extent of customer due diligence measures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction; and

(b) be able to demonstrate to his Supervisory Authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

You cannot avoid conducting CDD, but you can use a risk-based approach to determine the extent and quality of information required and the steps to be taken to meet the requirements.

You need only obtain information on the purpose and intended nature of your client's use of your services when you are in a business relationship with them. However, it's good practice to obtain such information to ensure you fully understand instructions and closely monitor the development of each retainer, even if it is for an occasional transaction or transactions below the threshold.

4.3.3 Methods of verification

Verification can be completed on the basis of documents, data and information which come from a reliable and independent source. This means that there are a number of ways you can verify a client's identity including:

- obtaining or viewing original documents
- conducting electronic verification as set out in the Electronic Identification Regulation or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the Gibraltar Regulatory Authority.
- obtaining information from other regulated persons

4.3.3.1 Independent source

You need an independent and reliable verification of your client's identity. This can include materials provided by the client, such as a passport.

Consider the cumulative weight of information you have on the client and the risk levels associated with both the client and the retainer.

You are permitted to use a wider range of sources when verifying the identity of the beneficial owner and understanding the ownership and control structure of the client. Often only the client or their representatives can provide you with such information. Apply the requirements in a risk-based manner to a level at which you are satisfied that you know who the beneficial owner is.

4.3.3.2 Documents

You should not ignore obvious forgeries, but you are not required to be an expert in forged documents.

4.3.3.3 Electronic verification

Electronic verification involves the use of electronic or digital (e.g. online) resources to verify the identity of a person, and should be used when a lawyer or a notary is unable to meet the client (or its officers and/or representatives) face to face. There are many providers of electronic verification services (e.g. Acuris Risk Intelligence Reports and World-Check) as well as electronic verification resources (e.g. websites and online search engines) which lawyers and notaries have the option to use in order to supplement face to face meetings and/or physical documents.

Electronic verification may only confirm that someone exists, and not that your client is the said person. You should consider the risk implications in respect of the particular retainer and be on the alert for information which may suggest that your client is not the person they say they are. You may mitigate risk by corroborating electronic verification with some other CDD material.

When choosing an electronic verification service provider, you should look for a provider who:

- has proof of registration with the Data Protection Commissioner to store personal data
- can link an applicant to both current and previous circumstances using a range of positive information sources
- accesses negative information sources, such as databases on identity fraud and deceased persons
- accesses a wide range of 'alert' data sources
- has transparent processes enabling you to know what checks are carried out, the results of the checks, and how much certainty they give on the identity of the subject
- allows you to capture and store the information used to verify an identity.

When using electronic verification, you are not required to obtain consent from your client, or clarify the resources you will use, but they must be informed that this check will take place.

While we believe electronic verification can be a sufficient measure for compliance with money laundering requirements, there may be circumstances where it will not be appropriate. For example, in the UK, the Council for Mortgage Lenders notes that electronic verification products may not be suitable for fraud prevention purposes, such as verifying that a person’s signature is genuine. Lawyers and notaries should always remain vigilant to the evolving nature of cybercrime and the dangers of identity theft and the impact such factors could have on their business and the reliability of electronic verification.

4.3.4 Reliance and outsourcing

Reliance has a very specific meaning within POCA and relates to the process under section 23 POCA where you rely on another regulated person to conduct CDD for you. You remain liable for any failure in the client being appropriately identified. Reliance does not include:

- accepting information from others to verify a client's identity when meeting your own CDD obligations
- electronic verification, which is outsourcing

You need

- the consent of the person on whom you rely for your reliance
- agreement that they will provide you with the CDD material upon request
- the identity of their supervisor for money laundering purposes. Consider checking the register for that Supervisory Authority, although a personal assurance of their identity may be sufficient where you have reasonable grounds to believe them.

We believe you should ask what CDD enquiries have been undertaken to ensure that they actually comply with POCA, because you remain liable for non-compliance. This is particularly important when relying on a person outside Gibraltar, and you should be satisfied that the CDD has been conducted to a standard compatible with 4MLD, taking into account the ability to use different sources of verification and jurisdictional specific factors. It may not always be appropriate to rely on another person to undertake your CDD checks and you should consider reliance as a risk in itself.

4.3.4.1 Reliance in Gibraltar

Under section 23(2) (a) and (b) POCA, you can only rely on the following persons in Gibraltar which are frequently referred to as 'eligible introducers' of business:

- A firm regulated by the Financial Services Commission, to whom the provisions of POCA apply;
- a person in the following professions who is supervised by a Supervisory Authority listed in Part 1 of Schedule 2:
    - auditor, insolvency practitioner, external accountant or tax adviser; or
    - independent legal professional

4.3.4.2 Reliance in an EEA state

Under section 23(2) (c) POCA, you can only rely on the following persons who carry on business in another EEA state:

- a credit or financial institution
- auditor, or EEA equivalent
- insolvency practitioner, or EEA equivalent
- external accountant
- tax adviser
- independent legal professional

They must also satisfy all of the following conditions:

- subject to mandatory professional registration recognised by law
- supervised for complying with money laundering obligations under section 2 of Chapter VI of the 4MLD.

A person will only be supervised in accordance with the 4MLD if the 4MLD has been implemented in the EEA state. You can check on the International Bar Association's website on the progress of implementation across Europe (www.anti-moneylaundering.org).

4.3.4.3 Reliance in other countries

Under section 23(2) (d) POCA, you can rely on the following persons who carry on business outside of the EEA unless they are established in a high risk third country:

- a credit or financial institution, or equivalent
- an auditor
- an insolvency practitioner
- an external accountant
- a tax adviser
- an independent legal professional.

They must also satisfy all of the following conditions:

- subject to mandatory professional registration recognised by law
- subject to requirements equivalent to those laid down in Section 2 of Chapter VI of the 4MLD

- supervised for complying with money laundering obligations to a standard equivalent to that under Section 2 of Chapter VI of the 4MLD.

On behalf of Member States, the European Commission publishes a list of countries considered to have equivalent AML/CTF systems.

- Consult the European Commission's List
- Consult the Joint Money Laundering Steering Group's ("JMLSG") guidance on equivalence (http://www.jmlsg.org.uk/)
- Consult a list of national money laundering legislation around the world, and whether it applies to lawyers.

As noted above, any third parties established in high risk third countries cannot be relied on at all by relevant financial businesses and are non-eligible introducers (section 23(1A) POCA), unless in a rare case the third party is a branch or majority-owned subsidiary of an obliged entity established in the European Union and adheres to group-wide policies and procedures in accordance with Article 45 of 4MLD (section 23(1B) POCA). High-risk third countries is to be interpreted as those countries on the list maintained by the GFSC referred to in chapter 4.9.3, and 'third country' or 'third countries' means a country or countries (or territory or territories) outside the EEA.

4.3.4.4 Passporting clients between jurisdictions

Some firms may have branches or affiliated offices ('international offices') in other jurisdictions and will have clients who utilise the services of a number of international offices. It is not considered proportionate for a client to have to provide original identification material to each international office.

Some firms may have a central international database of CDD material on clients to which they can refer. Where this is the case you should review the CDD material to be satisfied that CDD has been completed in accordance with the 4MLD. If further information is required, you should ensure that it is obtained and added to the central database. Alternatively, you could ensure that the CDD approval controls for the database are sufficient to ensure that all CDD is compliant.

Other firms may wish to rely on their international office to simply provide a letter of confirmation that CDD requirements have been undertaken with respect to the client. This will amount to reliance only if the firm can be relied upon under the terms of section 23 POCA and the CDD is completed in accordance with that section.

Finally, firms without a central database may wish to undertake their own CDD measures with respect to the client, but ask their international office to supply copies of the verification material, rather than the client themselves. This will not be reliance, but outsourcing.

It is important to remember that one of your international offices may be acting for a client who is not a PEP in that country, but will be when they are utilising the services of your office. As such, you will need to have in place a process for checking whether a person passported into your office is a PEP and, if so, undertake appropriate enhanced due diligence measures.

Gibraltar-based fee earners will have to undertake their own ongoing monitoring of the retainer, even if the international office is also required to do so.

4.3.5 Timing

4.3.5.1 When must CDD be undertaken?

Section 13(2) POCA requires you to verify your client's identity and that of any beneficial owner, before you establish a business relationship or carry out an occasional transaction.

Section 15 POCA provides that if you are unable to complete CDD in time, you cannot:

- carry out a transaction with or for the client through a bank account
- establish a business relationship or carry out an occasional transaction and additionally section 15 POCA provides that you must also:
- terminate any existing business relationship
- consider making a disclosure to the GFIU

Under section 16 POCA, to be read with Schedule 6 of POCA, evidence of identity is not required if a one-off transaction involves less than €15,000 or if two or more linked transactions involve less than €15,000 in total. This exception does not apply if there is any suspicion of money laundering or terrorist financing.

4.3.5.2 Exceptions to the timing requirement

There are several exceptions to the timing requirement and the prohibition on acting for the client.

However, you should consider why there is a delay in completing CDD, and whether this of itself gives rise to a suspicion which should be disclosed to the GFIU.

4.3.5.3 Normal conduct of business

Section 13(3) of POCA provides that verification may be completed during the establishment of a business relationship, (not an occasional transaction), where:

- it is necessary not to interrupt the normal conduct of business, and
- there is little risk of money laundering or terrorist financing occurring

you must complete verification as soon as practicable after the initial contact.

Consider your risk profile when assessing which work can be undertaken on a retainer prior to verification being completed.

Do not permit funds or property to be transferred or final agreements to be signed before completion of full verification.

If you are unable to conduct full verification of the client and beneficial owners, then the requirement to cease transactions contained in Section 15 of POCA will apply.

4.3.5.4 Ascertaining legal position

Section 15(2) POCA provides that the prohibition in 15(1) does not apply:

"to notaries, independent members of professions which are legally recognised and controlled, auditors and tax advisors who are in the course of ascertaining the legal position for their client or performing the task of defending or representing that client in, or concerning, legal proceedings, including advice on the institution or avoidance of proceedings."

The requirement to cease acting and consider making a report to the GFIU when you cannot complete CDD, does not apply when you are providing legal advice or preparing for or engaging in litigation or alternative dispute resolution.

This exception does not apply to transactional work, so take a cautious approach to the distinction between advice and litigation work, and transactional work.

4.4 Ongoing monitoring

Section 12 POCA requires that you conduct ongoing monitoring of a business relationship on a risk-sensitive and appropriate basis. Ongoing monitoring is defined as:

- scrutiny of transactions undertaken throughout the course of the relationship, (including where necessary, the source of funds), to ensure that the transactions are consistent with your knowledge of the client, their business and the risk profile and their source of funds.
- keeping the documents, data or information obtained for the purpose of applying CDD up-to-date. You must also be aware of obligations to keep clients' personal data updated under the DPA.

You are not required to:

- conduct the whole CDD process again every few years
- conduct random audits of files
- suspend or terminate a business relationship until you have updated data, information or documents, as long as you are still satisfied you know who
    - your client is, and keep under review any request for further verification material or processes to get that material
    - use sophisticated computer analysis packages to review each new retainer for anomalies

Ongoing monitoring will normally be conducted by fee earners handling the retainer, and involves staying alert to suspicious circumstances which may suggest money laundering, terrorist financing, or the provision of false CDD material.

For example, you may have acted for a client in preparing a will and purchasing a modest family home. They may then instruct you in the purchase of a holiday home, the value of which appears to be outside the means of the client's financial situation as you had previously been advised in earlier retainers. While you may be satisfied that you still know the identity of your client, as a part of your ongoing monitoring obligations it would be appropriate in such a case to ask about the source of the funds for this purchase. Depending on your client's willingness to provide you with such information and the answer they provide, you will need to consider whether you are satisfied with that response, want further proof of the source of the funds, or need to discuss making a disclosure to the GFIU with your appropriate person.

- To ensure that CDD material is kept up-to-date, you should consider reviewing it:
- when taking new instructions from a client, particularly if there has been a gap of over three years between instructions
- when you receive information of a change in identity details Relevant issues may include:
- the risk profile of the client and the specific retainer
- whether you hold material on transactional files which would confirm changes in identity
- whether electronic verification may help you find out if your clients' identity details have changed, or to verify any changes

4.5 Records

You are required to keep records of your CDD material, including electronic identification.

4.6 CDD on clients

Your firm will need to make its own assessments as to what evidence is appropriate to verify the identity of your clients. We outline a number of sources which may help you make that assessment.

4.6.1 Natural persons

A natural person's identity comprises a number of aspects, including their name, current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, and family circumstances.

Evidence of identity can include:

- identity documents such as passports and photo-card driving licences
- other forms of confirmation, including assurances from persons within the regulated sector or those in your firm who have dealt with the person for some time.
- Electronic documents

In most cases of face to face verification, producing a valid passport or photo-card identification should enable most clients to meet the AML/CTF identification requirements.

It is considered good practice to have either:

- one government document which verifies either name and address or name and date of birth; or
- a government document which verifies the client's full name and another supporting document which verifies their name and either their address or date of birth.

Where it is not possible to obtain such documents, consider the reliability of other sources and the risks associated with the client and the retainer. Electronic verification may be sufficient verification on its own as long as the service provider uses multiple sources of data in the verification process.

Where you are reasonably satisfied that an individual is nationally or internationally known, a record of identification may include a file note of your satisfaction about identity, usually including an address.

4.6.1.1 Individuals

Individuals perceived to present a low risk, a firm can satisfy the minimum customer identification documentation requirements by confirming the name and likeness by gaining sight of a document from a reliable and independent source which bears a photograph or from reliable and independent data sources.

For face-to-face customers a Gibraltar issued ID, Passport or local driving licence would easily meet this requirement. There is obviously a wide range of other documents which might be provided as evidence of identity. It is for each firm to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which might be easily forged or which can be obtained using false identities.

With identity theft becoming more of a concern, firms must remain vigilant to guard against the provision of false or stolen customer identification documentation being used to open and operate business relationships. Nothing in these Notes requires firms to put in place additional controls to check the veracity of the documents provided other than what would normally be required as part of good business practice. Firms however, may wish to use

electronic verification and other such processes to verify that customer supplied documents have not been forged.

The customer identification documentation, or data, obtained should demonstrate that a person of that name exists at the address given, and that the applicant for business is that person.

The address of the applicant for business can also generally be determined from the same document and if the customer's risk profile is low, there is no requirement to seek additional documentary evidence.

Where the document provided above does not contain details of the address, the address provided does not match that provided for the business relationship, or the customer risk profile presents a higher risk, a firm will need to conduct separate address verification.

A firm can easily satisfy this requirement using electronic sources of data without having to ask the customer. This is preferred as this also then satisfies the independent criteria as this is sought by the firm itself.

Care should be taken about applying this requirement too stringently, for example, where the address verification only shows up the spouse or family member of the applicant for business. In such cases the firm needs to document the linkage between the applicant for business and the person at the given address.

In respect of business relationships where the surname and/or address of the applicants for business differ, the name and address of all applicants, not only the first named, must be verified in accordance with the procedures set out above.

Any subsequent change to the customer's name, address, or employment details of which the institution becomes aware should be recorded as part of the know your customer process. Generally, this would be undertaken as part of good business practice and due diligence but also serves for money laundering and terrorist financing prevention.

The date of birth is important as an identifier in support of the name, and is helpful to assist law enforcement. Although there is no obligation to verify the date of birth, this provides an additional safeguard.

An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for due diligence measures as set out in these Notes.

4.6.1.2 Clients unable to produce standard documentation

Sometimes clients are unable to provide standard verification documents. The purpose of POCA is not to deny people access to legal services for legitimate transactions, but to mitigate the risk of legal services being used for the purposes of money laundering. You should consider whether the inability to provide you with standard verification is consistent with the client's profile and circumstances or whether it might make you suspicious that money laundering or terrorist financing is occurring.

Where you decide that a client has a good reason for not meeting the standard verification requirements, you may accept a letter from an appropriate person who knows the individual and can verify the client's identity.

4.6.2 Bodies Corporate

Where the applicant for business is a body corporate, the firm must ensure that;

(a) it fully understands the company's legal form,

(b) it understands the company's structure and ownership.

Corporate customers may be publicly accountable in several ways. Some public companies are listed on stock exchanges or other regulated markets, and are subject to market regulation and to a high level of public disclosure in relation to their ownership and business activities. Other public companies are unlisted, but are still subject to a high level of disclosure through public filing obligations. Private companies are not generally subject to the same level of disclosure, although they may often have public filing obligations. In their verification processes, firms should take account of the availability of public information in respect of different types of company.

The structure, ownership, purpose and activities of many corporates will be clear and understandable. Corporate customers can use complex ownership structures, which can increase the steps that need to be taken to be reasonably satisfied as to their identities; this does not necessarily indicate money laundering or terrorist financing. The use of complex structures without an obvious legitimate commercial purpose may, however, give rise to concern and increase the risk of money laundering or terrorist financing. Similarly, where a company has issued share warrants to bearer these must be kept immobilised under the control of a licensee. This is because the Guidance Notes cannot be complied with and due diligence in accordance with the Guidance Notes cannot be carried out, where beneficial ownership can change without the knowledge of the licensee.

Firms must put into place additional due diligence measures when establishing business relationships with non-Gibraltar registered companies, or companies with no direct business link to Gibraltar.

Such companies may be attempting to use geographic or legal complexities to interpose a layer of opacity between the source of funds and their final destination. In such circumstances, institutions should carry out effective checks on the source of funds and the nature of the activity to be undertaken during the proposed business relationship. This is particularly important if the corporate body is registered or has known links to countries without an effective AML/CFT regime. In the case of a trading company, a visit to the place of business may also be made to confirm the true nature of the business.

For corporates perceived to present a low risk, a firm can satisfy the minimum due diligence requirements by obtaining the following:

Either:

1. Obtaining a copy of the certificate of incorporation/certificate of trade or equivalent which should include the;

    - full name
    - registered number

OR

2. Performing a search in the country of incorporation which confirms the items in (1) above.

    - Registered office business addresses;
    - Copy of the latest report and accounts, is available and audited if applicable;
    - copy of the board resolution to open the relationship and the empowering authority for those who will operate any accounts;
    - Where the business relationship is being opened in a different name from that of the applicant, the institution should also make a search, or equivalent trading name search for the second name.

The following persons and beneficial owners as (i.e. individuals or legal entities) must also be identified in line with the above:

a. The beneficial owner(s) of the company as defined below (see chapter 4.7).

b. The shareholders of the company (if different from the beneficial owners) who own or control through direct or indirect ownership of a sufficient percentage of the shares or the voting rights or ownership interest in the company including through the bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards.

c. The natural person(s) who otherwise exercise control over the management of the company.

For corporate customers with multi-layered ownership structure, firms are required to document their understanding of the ownership and control structure of the natural and legal persons at each stage in the structure.

The key requirements are that such understanding is documented and must be obtained through reliable and verifiable sources. Such sources may include, for example, eligible introducers or group sources which the firm has determined and documented as reliable for these purposes or where documents have been obtained by the firm to demonstrate this.

The minimum level of detail to satisfy the documentation requirements required in these circumstances, for the intermediate legal entities, must include independently verifiable documents of the entity's existence and its registered shareholdings and management.

It will be on the basis of the firms' understanding of the ownership and control structure and the firm's assessment, of the Money Laundering and Terrorist Financing Risk presented by the structure, that the firm will determine which of the natural persons are beneficial owners of the applicant for business and whose identity needs to be verified in accordance with the above requirements.

It will be up to the firm itself to demonstrate that, in accordance with its risk assessment, the documentation obtained is sufficient to meet the requirements.

A simple example would be to obtain for each entity a comprehensive company search report from a reliable company registry or registered agent. However just as there are alternatives to a passport and utility bill, so there are alternatives to a company search and another example might be to obtain a set of consolidated financial statements that have been audited by a reliable firm of auditors and that show the group structure and ultimate controlling party.

4.6.2.1 Publicly Listed Companies

No further steps to verify identity over and above usual commercial practice, will normally be required where the applicant for business is known to be a listed company whose securities are admitted to trading on a regulated market within the meaning of Directive 2004/39/EC in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation.

4.6.3 Partnerships and unincorporated businesses

In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the institution, the identity of at least two partners or equivalent should be verified in line with the requirements for personal customers.

A partnership is not a separate legal entity, so you must obtain information on the constituent individuals.

Where partnerships or unincorporated businesses are:

- well-known, reputable organisations
- with long histories in their industries, and

- with substantial public information about them, their principals, and controllers the following information should be sufficient:
    - registered address, if any
    - trading address
    - nature of business

Other partnerships and unincorporated businesses which are small and have few partners should be treated as private individuals. Where the numbers are larger, they should be treated as private companies.

Where a partnership is made up of regulated professionals, it will be sufficient to confirm the firm's existence and the trading address from a reputable professional directory or search facility with the relevant professional body. Otherwise you should obtain evidence on the identity of at least the partner instructing you and one other partner, and evidence of the firm's trading address.

For a Gibraltar LLP, obtain information in accordance with the requirements for companies as outlined below.

4.6.4 Gibraltar or EU Credit or Financial Institutions

Verification of identity is not required when there are reasonable grounds for believing that the applicant for business is itself a financial institution in Gibraltar or an EU country, and is thus subject to the Money Laundering Directive. What constitutes reasonable grounds is not defined, but these might mean ensuring that the credit or financial institution does actually exist (e.g. that it is listed in the Bankers' Almanac, or is a member of a regulated or designated investment exchange); and that it is also regulated. In cases of doubt, the relevant regulator's list of institutions can be consulted. Additional comfort can also be obtained by obtaining from the relevant institution evidence of its authorisation to conduct financial and/or banking business.

For Gibraltar based firms, the GFSC publishes a list of regulated firms on its web-site (http://www.fsc.gi/regulated-entities). Verification that the applicant for business appears on these lists is sufficient to satisfy the minimum due diligence measures. Care, however, must be taken to distinguish between those that fall under the definitions of Credit Institutions or Financial Institutions, which fall under this exemption, and those that do not (e.g. company managers, professional trustees, insurance managers or insurance intermediaries).

Unregulated Gibraltar or EU credit or financial businesses should be subject to further verification in accordance with the procedures for companies or businesses

4.6.4 Other arrangements or bodies

4.6.4.1 Legal persons, trusts and similar legal arrangements

There are a wide variety of trusts, ranging from large, internationally active organisations subject to a high degree of public interest and quasi-accountability, through trusts set up under testamentary arrangements, to small, local trusts funded by small, individual donations from local communities, serving local needs.

In carrying out their risk assessments firms take account of the different money laundering or terrorist financing risks that trusts of different sizes and areas of activity present.

Most trusts and similar arrangements are not separate legal entities – it is the trustees collectively who are the customer. In these cases, the obligation to identify the customer attaches to the trustees, rather than to the trust itself. The purpose and objects of most trusts are set out in a trust deed.

In respect of trusts, the firm should obtain the following information:

a. full name of the trust;

b. nature and purpose of the trust (e.g., discretionary, testamentary, bare);
c. country of establishment;
d. identity of the settlor(s) or grantor(s);
e. identity of all trustees;
f. identity of any protector(s);
g. where the beneficiaries have already been determined, the identity of the natural person(s);
h. where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; and
i. any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.

In the case of fixed interest trusts, where beneficiaries have been pre-determined (e.g. the children of settlor) and they have a fixed interest, which may be contingent (50% income upon attaining age of 21) or otherwise (50% of income); the identity of those beneficiaries must clearly be determined at the outset.

The position becomes a less clear in the case of discretionary trusts (e.g. children of settlor may receive such percentage of the income of the trust as the trustee shall determine in its sole discretion). In such cases the formal documentation of a beneficiary's identity during the lifetime of the trust need only be conducted prior to the distribution of trust assets (if and when beneficiaries are determined at the discretion of the trustee) and not when the trust is established.

Where a trustee is itself a regulated entity, or a publicly quoted company, or other type of entity, the identification procedures that should be carried out should reflect the standard approach for such an entity.

Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

Some consideration should be given as to whether documents relied upon are forged. In addition, if they are in a foreign language, appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity.

Firms must make appropriate distinction between those trusts that serve a limited purpose (such as inheritance tax planning) or have a limited range of activities and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

For trusts presenting a lower money laundering or terrorist financing risk, the minimum due diligence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money laundering or terrorist financing risk. Also, some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering.

Where a trust is assessed as carrying a higher risk of money laundering or terrorist financing, the firm must seek additional information in order to satisfy the customer identification documentation.

4.6.4.2 Clubs and societies

Where an application is made on behalf of a club or society, firms should make appropriate distinction between those that serve a limited social or regional purpose and those where the activities and connections are more sophisticated, or are geographically based and/or with financial links to other countries.

For many clubs and societies, the money laundering or terrorist financing risk will be low.

The following minimum due diligence must be conducted on clubs and societies:

a) Full name of the club/society
b) Legal status of the club/society
c) Purpose of the club/society
d) Names of all officers

The firm should verify the identities of the officers of a club or society who have authority to operate an account or to give instructions concerning the use or transfer of funds or assets.

Firms should take appropriate steps to be reasonably satisfied that the person the firm is dealing with is properly authorised by the customer and is who he says he is.

4.7 CDD on a beneficial owner

The term "beneficial owner" is to be interpreted throughout these Notes in accordance with section 1A of POCA and as meaning the following;

> *"The person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted and includes, at least, the following;*
>
> *in the case of a corporate entity;*
>
> *1. the natural person(s) who ultimately own or control a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information;*
> *2. if no person can be identified, after having exhausted all possible means and provided there are no grounds for suspicion, or if there is any doubt that the person identified is the beneficial owner, firms will be expected to at least identify the natural person who holds the position of senior managing official, and shall maintain records of the actions taken in order to identify the beneficial ownership;*
>
> *in the case of legal arrangements such as trusts which administer and distribute funds;*
>
> *3. the settlor(s);*
> *4. the trustee(s);*
> *5. the protector(s), if any;*
> *6. where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement;*
> *7. where the individuals that benefit from the trust have yet to be determined, the class of persons in whose main interest the trust is set up or operates;*
> *8. any other natural person(s) exercising control over 25% or more of the property of the trust by means of direct or indirect ownership or by other means;*
>
> *in the case of a legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions by exercising control over 25% or more of the property of the foundation or legal arrangement or other entity by means of direct or indirect ownership or by other means."*

4.7.1 General comments

When conducting CDD on a client, you will need to identify any beneficial owners within the meaning of section 1A of POCA. Note that this definition is to be read with sections 1B and

1C POCA. Section 1B clarifies that a shareholding of 25% plus one share or an ownership interest of more than 25% (where there are no "shares", such as in trusts) in the customer held by a natural person shall be an indication of "direct" ownership in the definition referred to above. "Indirect ownership" works in the same way, but one or more persons are interposed between the same natural person who ultimately controls more than 25% of the corporate, trust, foundation or other form of legal entity (i.e. your client).

You should also note control exercised "by other means" (in other words other than by having a 25% plus one share or 25% beneficial ownership via direct or indirect ownership). This has a much broader meaning and POCA makes reference in section 1B to Directive

2013/34/EU[3] (the "Accounting Directive"), and Article 22(1) to (5) which deal with, amongst other matters, the concepts of:

- "right to exercise a dominant influence"
- "[a subsidiary being] managed on a unified basis [by a parent undertaking]"
- "the right to appoint or remove a majority of the members of the administrative, management or supervisory body of another undertaking (a subsidiary undertaking)"

Section 1B is not meant to provide an exhaustive list, as it uses the expression "inter alia" before referring to the Accounting Directive. Ultimately the key appears to be that "all possible means" must be exhausted in order to attempt to uncover the beneficial owner, and if this cannot be done the key management person should be identified, where there is still lack of clarity, a natural person must be arrived at, unless there is a listed entity controlling the client directly or indirectly.

As well as exhausting all possible steps to try and identify the ultimate beneficial owner, firms are advised to keep a clear record of all actions taken in order to prove that all possible means have indeed been exhausted.

To identify the beneficial owner, obtain at least their name and record any other identifying details which are readily available. You may decide to use records that are publicly available, ask your client for the relevant information or use other sources.

To assess which identity verification measures are needed, consider the client's risk profile, any business structures involved and the proposed transaction.

The key is to understand the ownership and control structure of the client. A prudent approach is best, monitoring changes in instructions, or transactions which suggest that someone is trying to undertake or manipulate a retainer for criminal ends. Simply ticking boxes is unlikely to satisfy the risk-based approach.

Appropriate verification measures may include:

- a certificate from your client confirming the identity of the beneficial owner
- a copy of the trust deed, partnership agreement or other such document
- shareholder details from an online registry
- the passport of, or electronic verification on, the individual
- other reliable, publicly available information

4.7.2 Assessing the risk

Issues you may consider when assessing the risk of a particular case include:

- why your client is acting on behalf of someone else

[3] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC.

- how well you know your client
- whether your client is a regulated person
- the type of business structure involved in the transaction
- where the business structure is based
- the AML/CTF requirements in the jurisdiction where it is based
- why this business structure is being used in this transaction
- how soon property or funds will be provided to the beneficial owner

Only in rare cases will you need to verify a beneficial owner to the same level that you would a client.

When conducting CDD on beneficial owners within a corporate entity or arrangement, you must:

- understand the ownership and control structure of the client as required by Section 10(b) POCA
- identify the specific individuals listed in Chapter 1, Article 3(6) of the 4MLD.

The level of understanding required depends on the complexity of the structure and the risks associated with the transaction. For example, it may be sufficient to review the trust deed or partnership arrangement and discuss the issue with your client. In the case of a company, you may obtain a company structure chart from your client directly, their website or their annual reports.

It is vital to understand in what capacity your client is instructing you to ensure that you are identifying the correct beneficial owners.

If for example you are acting for Bank A, which is a corporate entity, to purchase new premises for Bank A, then it would be the shareholders and controllers of Bank A who are the beneficial owners. However, if Bank A is a trustee for XYZ Trust and they have instructed you to sell trust property, then Bank A is instructing you on behalf of the arrangement which is XYZ Trust in their capacity as trustee. The beneficial owners in that transaction will be those with specified interests in and/or control of the XYZ Trust.

4.7.3 Agency

Chapter 1, Article 3(6) of the 4MLD suggests a beneficial owner generally means any individual who ultimately owns or controls the client or on whose behalf a transaction or activity is being conducted. Section 10A of POCA says that, in identifying a beneficial owner, relevant financial businesses must also verify that any person purporting to act on their behalf is so authorised and identify and verify the identity of that person. Although not defined in POCA, a person purporting to act on behalf of the beneficial owner that is so authorised to act can be referred to as his ‘Agent’ for the purposes of these Guidance Notes.

In these cases, it is presumed the client is himself the beneficial owner, unless the features of the transaction indicate they are acting on someone else's behalf. So, you do not have to proactively search for beneficial owners, but to make enquiries when it appears the client is not the beneficial owner.

Situations where a natural person may be acting on behalf of someone else as his Agent include:

- exercising a power of attorney. The document granting power of attorney may be sufficient to verify the beneficial owner's identity.
- acting as the deputy, administrator or insolvency practitioner. Appointment documents may be sufficient to verify the beneficial owner's identity.
- an appointed broker or other agent to conduct a transaction. A signed letter of appointment may be sufficient to verify the beneficial owner's identity.

Additionally, you should consider corporate persons, such as law firms and other professional advisers, intermediaries or referrers of business. Steps should also be taken to verify that persons claiming to be from such firms are actually employees or otherwise duly authorised to transact and conduct business on behalf of such firms. If you have verified their positions from websites or other documents, have visited their offices or have confirmed they and/or their firm is/are licensed by a regulator in a reputable jurisdiction, it may be sufficient to establish the identity and the authority of these types of Agents, and such Agents' representatives.

You should be alert to the possibility that purported agency relationships are actually being utilised to facilitate a fraud. Understanding the reason for the agency, rather than simply accepting documentary evidence of such at face value, will assist to mitigate this risk. Where a client or retainer is higher risk, you may want to obtain further verification of the beneficial owner's identity in line with the suggested CDD methods to be applied to natural persons.

4.7.4 Companies

Chapter 1, Article 3(6) (a) of the 4MLD defines the beneficial owner of a body corporate as meaning:

Any natural person(s) who:

- as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25 per cent of the shares or voting rights in the body, or
- as respects any body corporate, otherwise exercises control over the management of the body

This provision does not apply to a company listed on a regulated market

4.7.4.1 Shareholdings

You should make reasonable and proportionate enquiries to establish whether beneficial owners exist and, where relevant as determined by your risk analysis, verify their identity.

These may include:

- getting assurances from the client on the existence and identity of relevant beneficial owners
- getting assurances from other regulated persons more closely involved with the client, particularly in other jurisdictions, on the existence and identity of relevant beneficial owners
- if, you have exhausted all possible means and have no grounds for suspicion, no person has been identified as the ultimate beneficial owner or if there is any doubt that the person identified is the ultimate beneficial owner, the natural person who holds the position of senior managing official shall be the person to whom CDD is applied, keeping records of the actions taken as well as any difficulties encountered during the verification process
- conducting searches on the relevant online registry
- obtaining information from a reputable electronic verification service

Where the holder of the requisite level of shareholding of a company is another company, apply the risk-based approach when deciding whether further enquiries should be undertaken.

4.7.5 A proportionate approach

It would be disproportionate to conduct independent searches across multiple entities at multiple layers of a corporate chain to see if, by accumulating very small interests in different

entities, a person finally achieves more than a 25 per cent interest in the client corporate entity. You must simply be satisfied that you have an overall understanding of the ownership and control structure of the client company.

Voting rights are only those which are currently exercisable and attributed to the company's issued equity share capital.

4.7.6 Companies with capital in the form of bearer shares

These pose a higher laundering risk as it is often difficult to identify beneficial owners and such companies are often incorporated in jurisdictions with a lower standard of AML/CTF laws and regulations. You should adopt procedures to establish the identities of the holders and material beneficial owners of such shares and ensure you are notified whenever there is a change of holder and/or beneficial owner. This may be achieved by:

- requiring that the shares be held by a regulated person
- getting an assurance that either such a regulated person or the holder of the shares will notify you of any change of records relating to the shares

4.7.7 Control

A corporate entity can also be subject to control by persons other than shareholders. Such control may rest with those who have power to manage funds or transactions without requiring specific authority to do so, and who would be in a position to override internal procedures and control mechanisms.

You should remain alert to anyone with such powers while you are obtaining a general understanding of the ownership and control structure of the corporate entity. Further enquiries are not likely to be necessary. Monitor situations within the retainer where control structures appear to be bypassed and make further enquiries at that time.

4.8 Simplified due diligence

Section 16 POCA permits simplified due diligence to be undertaken in certain circumstances, for example, in the potentially lower risk situations set out in Schedule 6 of POCA (copied further below).

4.8.1 Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinising transactions, based on a reasonable monetary threshold.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

4.9.2 Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Thresholds

4.8.3 The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Financial transactions above the designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

Ongoing due diligence

4.8.4 Financial institutions should be required to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of customers.

(1) Customer risk factors-

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

(b) public administrations or enterprises;

(c) customers that are resident in geographical areas of lower risk as set out in point (3).

(2) Product, service, transaction or delivery channel risk factors-

(a) life insurance policies for which the premium is low;

(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;

(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money).

(3) Geographical risk factors-

(a) Member States;

(b) third countries having effective AML/CFT systems;

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;

(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

4.9 Enhanced due diligence

Section 17 POCA provides that you will need to apply enhanced due diligence on a risk-sensitive basis where:

- any of the cases referred to in Articles 19 to 24 of 4MLD applies
- you are dealing with natural persons or legal entities established in third countries identified by the European Commission as high risk third countries. In such cases your must-

  (a) obtain additional information on the customer and on the beneficial owners

  (b) obtain additional information on the intended nature of the business relationship

  (c) obtain information on the source of funds and source of wealth of the customer and of the beneficial owners

  (d) obtain information on the reasons for the intended or performed transactions

(e) obtain the approval of senior management for establishing or continuing the business relationship

(f) conduct enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

- you, as a relevant financial business, have identified a case of higher risk or such cases are identified by the Minister by notice in the Official Gazette (to date the Minister has not published such a list of high-risk cases).

The cases referred to in Articles 19 to 24 of 4MLD are:

- cross-border correspondent relationships with a third-country respondent institution (Article 19),
- the client is a PEP (Article 20)
- when beneficiaries of a life or other investment-related insurance policy and/or, where required, the beneficial owner of the beneficiary are PEPs (Article 21)
- where the client is a former PEP and no longer entrusted with a prominent public function, during the period of 12 months from the time he ceases to be a PEP (Article 22)
- clients are family members of PEPs (Article 23)
- correspondent banking relationships with shell banks (see section 22(4) POCA for a definition of shell bank) (Article 24)

In assessing cases of higher risks, relevant financial businesses must at least take into account of the factors of potentially higher-risk situations set out in Schedule 7, which reproduces Annex III to the Money Laundering Directive. These are split into:

- Customer risk factors
- Product, service, transaction or delivery channel risk factors
- Geographical risk factors

In accordance with section 17(3) POCA, you must also examine as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose, and in particular, a relevant financial business shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

In applying the risk-based approach to the situation you should consider whether it is appropriate to:

- seek further verification of the client or beneficial owner's identity
- obtain more detail on the ownership and control structure of the client
- request further information on the purpose of the retainer or the source of the funds, and/or
- conduct enhanced ongoing monitoring

4.9.0 Directions to Undertake EDD

The supervisory authority may give a direction under subsection 17(7) of POCA to the relevant financial business to apply one or more of the additional mitigating measures set out in Schedule 8 to persons and legal entities carrying out transactions involving high risk third countries.

These include;

- enhanced due diligence
- ongoing monitoring

- systematic reporting; or
- limiting or ceasing business

See POCA for the full list of measures under Schedule 8.

4.9.1 Non face-to-face clients

Any mechanism through which the customer is allowed to interact with a firm in a non-direct manner increases the firm's exposure to risk. Not only does this allow for third parties to have access to assets or property through impersonation but also disguise the true owner of that property by, for example, provision of false identification documentation.

Firms must put into place systems of control that appropriately address the risks posed by non-face to face contact for customers either at the opening of the business relationship or through the operation of that relationship.

Additional controls are required in respect of non-face-to-face customers; for example, applying one or more of the following measures of control:

a) ensuring that the customer's identity is established by additional documents, data or information; or
b) supplementary measures to verify the documents supplied, or requiring an eligible introducer to certify the customer identification documents be required; or
c) ensuring that the first payment of the operation is carried out through an account in the customer's name at a credit institution ; or
d) Landline telephone contact with the customer on a number which has been verified; or
e) Sending information or documents required to operate the business relationship to a physical address that has been verified.

A common mechanism adopted by many firms is to permit the use of certified customer identification documents provided in lieu of having had sight of the originals.

In drawing up the list of persons approved to certify identification documents for a firm, the appropriate person will need to provide documentary evidence of the following:

(a) That the person;

  i. adheres to ethical and/or professional standards; and

  ii. is readily contactable; and

  iii. exercises his or her profession or vocation in a jurisdiction with effective anti-money laundering measures; and

(b) The MLRO has obtained senior management agreement to permit such a person from certifying documents for these purposes.

There is obviously a wide range of documents which might be provided as evidence of identity. It is for each firm to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

4.9.2 Politically exposed persons

The term "politically exposed persons" ("**PEP**" or "**PEPs**") is defined in Article 3(9) of the 4MLD as:

> *"natural person who is or who has been entrusted with prominent public functions and includes the following:*

(a) heads of state, heads of government, ministers and deputy or assistant ministers;

(b) members of parliament or of similar legislative bodies;

(c) members of the governing bodies of political parties;

(d) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

(e) members of courts of auditors or of the boards of central banks;

(f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;

(g) members of the administrative, management or supervisory bodies of State-owned enterprises;

(h) directors, deputy directors and members of the board or equivalent function of an international organisation

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials"

This definition has been transferred verbatim into section 20A of POCA, which does not distinguish between domestic and foreign PEPs. When a firm is considering establishing a business relationship with a PEP, additional considerations in section 20 POCA must be taken into account in addition to the CDD requirements contained in sections 10 to 13 POCA; specifically, firms must:

"(a) have approval from senior management for establishing or continuing the business relationship with that person;

(b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and

(c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship."

Firms must also consider that the requirements above apply in exactly the same manner to 'family members' and 'persons known to be close associates' as though such persons are themselves PEPs.

'family members' shall include the following:

(a) a spouse, or a person considered to be equivalent to a spouse;

(b) children and their spouses or persons considered to be equivalent to a spouse;

(c) parents.

'persons known to be close associates' shall include the following (and for the purpose of decided whether a person is a known close associate of a PEP, a relevant financial business need only have regard to information which is in its possession or is publicly known):

(a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP;

(b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a PEP.

Without prejudice to the application, on a risk-sensitive basis, of enhanced customer due diligence measures, where a person has ceased to be entrusted with a prominent public function for a period of at least one year, firms shall not be obliged to consider such a person

as politically exposed in accordance with section 20B of POCA, provided that the person is deemed to pose no further risk specific to politically exposed persons.

The concerns relating to this type of risk are mitigated by having adequate processes through which a firm can determine the source of income or wealth.

Specific risk-based measures need to be adopted to reduce the risks inherent in dealing with PEPs.

The systems of control that firms must adopt to reduce the risks associated with establishing and maintaining business relationships with PEPs are that:

a. The firm must establish and document a clear policy and internal guidelines, procedures and controls regarding such business relationships;
b. Maintain an appropriate risk management system to determine whether a potential customer or an existing customer is a PEP;
c. Decisions to enter into business relationships with PEPs to be taken only by senior management;
d. Business relationships which are known to be related to PEPs must be subject to proactive monitoring of the activity on such accounts.

The monitoring of the accounts is necessary so that any changes are detected, and consideration can be given as to whether such change suggests corruption or misuse of public assets. This includes close scrutiny of receipts of large sums from government bodies, state owned activities, or governments and central bank accounts.

Recital 33 of 4MLD provides the context that just because a person is PEP does not mean they should automatically be refused as a new business relationship:

> *"(33) The requirements relating to politically exposed persons are of a preventive and not criminal nature, and should not be interpreted as stigmatising politically exposed persons as being involved in criminal activity. Refusing a business relationship with a person simply on the basis of the determination that he or she is a politically exposed person is contrary to the letter and spirit of this Directive and of the revised FATF Recommendations."*

4.9.3 natural persons or legal entities established in third countries

Enhanced due diligence is also required when transacting business with third countries, and in particular those countries where there is a higher risk of money laundering.

The Financial Action Taskforce regularly provides statements on unsatisfactory money laundering controls in overseas jurisdictions. The Financial Services Commission regularly updates a list of FATF High Risk jurisdictions by way of a newsletter on its website (http://www.gfsc.gi/downloads?section=8&type=1). .

You must undertake enhanced due diligence and enhanced ongoing monitoring when acting in relation to transactions involving these jurisdictions.

4.9.4

New technologies

When conducting Relevant Financial Business, legal professionals should be aware of money laundering or terrorist financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products, for example Distributed Ledger Technology (DLT), Virtual Assets (VA) and any other new technologies identified by the National Coordinator for Anti-Money Laundering and Combatting Terrorist Financing (NCO), whether in the National Risk Assessment or other publication. Legal

professionals should take appropriate measures to identify, manage and mitigate those risks and act strictly in accordance with PoCA, the Guidance Notes and international standards.

4.10 Existing clients

Section 11(2) POCA states you must apply CDD measures to an existing customer at other appropriate times and on a risk-sensitive basis.

You do not have to ensure all existing clients have been identified and verified by the date of entry of these Guidance Notes, nor update all current identification in accordance with the new requirements by this date.

Factors that may trigger a need for CDD include:

- a gap in retainers of three years or more
- a client instructing on a higher risk retainer
- where you develop a suspicion of money laundering or terrorist financing by
    - the client
    - an existing high-risk client

For all clients, you should ensure ongoing monitoring of the business relationship to identify any suspicious activity.

When conducting CDD on existing clients or a subsidiary of an existing client, you may consider information already on your files which would verify their identity or publicly available information to confirm the information you hold, rather than approaching the client to provide that information initially. It may be appropriate for a fee earner or partner who has known the client for long time to place a certificate on the file providing an assurance as to identity.

4.11 FATF counter measures

Your CDD measures should, following a risk-based approach, be able to ascertain whether your client is subject to the restrictions or directions listed below.

You should also be able to ascertain whether beneficial owners or the intended recipient of funds from a transaction you are undertaking are subject to the restrictions or directions listed below, where there is a higher risk of money laundering or terrorist financing.

You should assess each case on its merits. However, examples of higher risk situations may include transactions with:

- complex corporate entities in jurisdictions where there is a high risk of terrorist funding
- senior politically exposed persons from jurisdictions which are subject to sanctions

4.11.1 FATF Counter-measures

The Minister may, under Section 24 of POCA direct relevant financial businesses to;

(a) not enter into a business relationship ;
(b) not carry out an occasional transaction ; or
(c) not to proceed any further with a business relationship or occasional transactions;

With a person who is situated or incorporated in a non-EEA State or Territory to whom the FATF has decided to apply countermeasures.

4.11.12 Financial Restrictions – General

HM Government of Gibraltar imposes financial restrictions on persons and entities following their designation by the United Nations and/or European Union. Gibraltar also operates a domestic counter-terrorism regime, where the government decides to impose financial restrictions on certain persons and entities.

Subsidiary legislation is issued for each financial restriction in force. An order will be made freezing the assets of a person or entity, where a financial restriction is imposed. It is unlawful to make payments to or allow payments to be made to that designated person or entity.

4.11.2 Restrictions against Al-Qaida and terrorism

The Al Qaida and Taliban (United Nations Measures) Order 2006 and the Terrorism (United Nations Measures) Order 2009 create specific offences for providing funds or economic resources to terrorists.

4.12 Further Guidance

Articles 17, 18(4) and 48(10) 4MLD require European Supervisory Authorities to establish certain guidelines in the following areas:

- "the risk factors to be taken into consideration and the measures to be taken in situations where simplified customer due diligence measures are appropriate." (Article 17).
- the risk factors to be taken into consideration and the measures to be taken in situations where enhanced customer due diligence measures are appropriate (Article 18(4))
- the characteristics of a risk-based approach to supervision and the steps to be taken when conducting supervision on a risk-based basis (Article 48(10)).

Guidance in each of the areas has been issued by the ESAs, which in this case has been the Joint Committee of the three European Supervisory Authorities (EBA, EIOPA and ESMA – ESAs). Two guidance notes were published on 16 November 2016 and 26 June 2017 in line with 4MLD:

1. the guidance on simplified and enhanced CDD measures (Articles 17 and 18(4)) is accessible at: https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

2. the guidance on the characteristics of a risk based approach to supervision and the steps to be taken when conducting supervision on a risk-based basis (article 48(10)), is accessible at: https://esas-joint-committee.europa.eu/Publications/Guidelines/Final_RBSGL_for_publication_20161115.pdf

Each of these Articles of 4MLD further state that:

"*specific account shall be taken of the nature and size of the business, and, where appropriate and proportionate, specific measures shall be laid down*",

It should therefore be borne in mind that the ESAs' guidance documents referred to above have to be read in the context of the nature and size of the relevant financial business, and actions taken should always remain proportionate.

The guidance at Article 18(4) is referred to at section 17 POCA, but it is not relevant to independent legal professionals because it is aimed at credit and financial institutions.

As for the guidance at Article 48(10), this is addressed to competent authorities of member states and again is not relevant.

Nevertheless, this has been cited here for the avoidance of doubt and to ensure that independent legal professionals are aware of what guidance applies and does not apply to them.

Chapter 5 Money Laundering Offences

5.1 General comments

POCA introduced a single set of money laundering offences applicable throughout Gibraltar to the proceeds of all crimes. It also creates a disclosure regime, which makes it an offence not to disclose knowledge or suspicion of money laundering, but also permits persons to be given consent in certain circumstances to carry out activities which would otherwise constitute money laundering.

5.2 Application

POCA applies to all lawyers and notaries, although some offences apply only to persons within a relevant financial business, or appropriate persons.

5.3 Mental elements

The mental elements which are relevant to offences under Part 2 of POCA are:

- knowledge
- suspicion
- reasonable grounds for suspicion

These are the three mental elements in the actual offences, although the third one only applies to offences relating a relevant financial business. There is also the element of belief on reasonable grounds in the foreign conduct defence to the money laundering offences. A person will have a defence to a principal offence if they know or believe on reasonable grounds that the criminal conduct involved was exempt overseas criminal conduct.

For the principal offences of money laundering the prosecution must prove that the property involved is criminal property. This means that the prosecution must prove that the property was obtained through criminal conduct and that, at the time of the alleged offence, you knew or suspected that it was.

For the failure to disclose offences, where you are acting in a relevant financial business, you must disclose if you have knowledge, suspicion or reasonable grounds for suspicion.

These terms for the mental elements in the offences are not terms of art; they are not defined within POCA and should be given their everyday meaning. However, case law has provided some guidance on how they should be interpreted.

5.3.1 Knowledge

Knowledge means actual knowledge. There is some suggestion that wilfully shutting one's eyes to the truth may amount to knowledge. However, the current general approach from the criminal courts is that nothing less than actual knowledge will suffice.

5.3.2 Suspicion

The term 'suspects' is one which the court has historically avoided defining; however, because of its importance in English criminal law, some general guidance has been given. In the case of *Da Silva* [1996] EWCA Crim 1654, which was prosecuted under the previous money laundering legislation, Longmore LJ stated:

> *'It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.'*

There is no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief, but at least extending beyond speculation.

The test for whether you hold a suspicion is a subjective one.

If you think a transaction is suspicious, you are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. You may have noticed something unusual or unexpected and after making enquiries, the facts do not seem normal or make commercial sense. You do not have to have evidence that money laundering is taking place to have suspicion.

Chapter 11 of these Guidance Notes contains a number of standard warning signs which may give you a cause for concern; however, whether you have a suspicion is a matter for your own judgement. To help form that judgement, consider talking through the issues with colleagues or with the Bar Council. You could also take legal advice. Listing causes for concern can also help focus your mind.

If you have not yet formed a suspicion but simply have cause for concern, you may choose to ask the client or others more questions. This choice depends on what you already know, and how easy it is to make enquiries.

If you think your own client is innocent but suspect that another party to a transaction is engaged in money laundering, you may still have to consider referring your client for specialist advice regarding the risk that they may be a party to one of the principal offences.

5.3.3 Reasonable grounds to suspect

The issues here for the lawyer or notary conducting regulated activities are the same as for the mental element of suspicion, except that it is an objective test. Were there factual circumstances from which an honest and reasonable person, engaged in a business in the regulated sector should have inferred knowledge or formed the suspicion that another was engaged in money laundering?

5.4 Principal Money laundering offences/provisions (and duties to disclose)

5.4.1 General comments

Money laundering offences assume that a criminal offence has occurred in order to generate the criminal property which is now being laundered. This is often known as a predicate offence. No conviction for the predicate offence is necessary for a person to be prosecuted for a money laundering offence.

When considering the principal money laundering offences, be aware that it is also an offence to conspire or attempt to launder the proceeds of crime, or to counsel, aid, abet or procure money laundering.

The principal money laundering offences are the offences under sections 2(1), 3(1) and 4(1) POCA, but do note that POCA has a wide array of other offences (see chapter 9.3).

5.4.2 Section 2(1) POCA - Arrangements

A person commits an offence if he enters into, or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

5.4.2.1 What is an arrangement?

Arrangement is not defined in POCA. The arrangement must exist and have practical effects relating to the acquisition, retention, use or control of property by or on behalf of another person.

An agreement to make an arrangement will not always be an arrangement. The test is whether the arrangement does in fact, in the present and not the future, have the effect of facilitating the acquisition, retention, use or control of criminal property by or on behalf of another person.

5.4.2.2 What is not an arrangement?

Bowman v Fels (Bar Council and others intervening) [2005] EWCA Civ 226 held that section 328 of the UK Proceeds of Crime Act 2002 ("UKPOCA") (the equivalent of section 2(1) POCA) does not cover or affect the ordinary conduct of litigation by legal professionals, including any step taken in litigation from the issue of proceedings and the securing of injunctive relief or a freezing order up to its final disposal by judgment.

The dividing of assets in accordance with the judgment, including the handling of the assets which are criminal property, is not an arrangement. Further, settlements, negotiations, out of court settlements, alternative dispute resolution and tribunal representation are not arrangements. However, the property will generally still remain criminal property and you may need to consider referring your client for specialist advice regarding possible offences they may commit once they come into possession of the property after completion of the settlement.

The recovery of property by a victim of an acquisitive offence will not be committing an offence under either section 2(1) or section 3 of POCA

5.4.2.3 Sham litigation

Sham litigation created for the purposes of money laundering remains within the ambit of section 2(1) POCA. Our view is that shams arise where an acquisitive criminal offence is committed and settlement negotiations or litigation are intentionally fabricated to launder the proceeds of that separate crime.

A sham can also arise if a whole claim or category of loss is fabricated to launder the criminal property. In this case, money laundering for the purposes of POCA cannot occur until after execution of the judgment or completion of the settlement.

5.4.2.4 Entering into or becoming concerned in an arrangement

To enter into an arrangement is to become a party to it.

To become concerned in an arrangement suggests a wider practical involvement such as taking steps to put the arrangement into effect.

Both entering into, and becoming concerned in, describe an act that is the starting point of an involvement in an existing arrangement.

Although the Court did not directly consider the conduct of transactional work, its approach to what constitutes an arrangement under section 2(1) POCA provides some assistance in interpreting how that section applies in those circumstances.

Our view is that *Bowman v Fels* (cited above) supports a restricted understanding of the concept of entering into or becoming concerned in an arrangement, with respect to transactional work. In particular:

- entering into or becoming concerned in an arrangement involves an act done at a particular time
- an offence is only committed once the arrangement is actually made, and

- preparatory or intermediate steps in transactional work which does not itself involve the acquisition, retention, use or control of property will not constitute the making of an arrangement under section 2(1) POCA

If you are doing transactional work and become suspicious, you have to consider:

- whether an arrangement exists and, if so, whether you have entered into or become concerned in it or may do so in the future
- if no arrangement exists, whether one may come into existence in the future which you may become concerned in

5.4.3 Section 3(1) POCA - Acquisition, Use or Possession

A person commits an offence if he acquires, uses or has possession of criminal property, and for the purposes of section 3(1) POCA, having possession of any property shall be taken to be doing an act in relation to it.

5.4.4 Section 4(1) POCA – Concealing

A person commits an offence if he conceals, disguises, converts, or transfers criminal property, or removes criminal property from Gibraltar.

A person will also commit an offence under section 4 POCA if, knowing or having reasonable grounds to suspect that any property is or in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct he conceals, disguises, converts or transfers that criminal property, or removes the criminal property from Gibraltar.

Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights connected with it.

5.5 Defences to principal money laundering offences

These are your possible defences to a principal money laundering offence.

5.5.1 Sections 2, 3 and 4 POCA Defences – the general defences

You have a defence to any offence under sections 2, 3 and 4 POCA if:

- you make an authorised disclosure and receive appropriate consent, deemed consent or negative consent as defined below
- you intended to make such a disclosure but had a reasonable excuse for not doing so
- you commit a prohibited act under any of these sections but you do this in carrying out a function relating to enforcement of POCA or other relevant legislation relating to criminal conduct or benefit from criminal conduct

5.5.1.1 appropriate consent/DAML

If you have a suspicion that a retainer you are acting in will involve dealing with criminal property, you can make a disclosure to the GFIU via your appropriate person (i.e. the nominated officer or MLRO) and seek consent/DAML to undertake the further steps in the retainer which would constitute a money laundering offence.

Once you or your appropriate person has made a disclosure to the GFIU a few potential scenarios can occur:

- Within 14 working days (starting with the first working day after the disclosure is made) the GFIU grants appropriate consent/DAML to the doing of a prospective prohibited act (**Scenario 1**)
- The GFIU notifies you / your appropriate person of its refusal of consent (at any time) (**Scenario 2)**

- After 14 working days (starting with the first working day after the disclosure is made) the GFIU does not notify you / your appropriate person of its refusal of consent (**Scenario 3**)
- 60 working days elapse since the GFIU notifies you / your appropriate person of its refusal of consent, (starting with the first working day after the GFIU notifies its refusal of consent), known as the moratorium period (**Scenario 4**)

Having received consent from the GFIU, if you act in contravention of the money laundering offence you will not have committed an offence under sections 2(1), 3(1) or 4(1) POCA. But there are situations where even if you hear nothing from the GFIU, you are still taken to have obtained consent. If this happens, the effect is that **you are allowed to proceed with the transaction** and will be protected by a DAML.

Consent can be split into three categories:

- Appropriate consent, as defined in section 4A(1) POCA
- Deemed consent, which is not specifically defined but created under sections 4A(3) and 4A(4) POCA
- Negative consent, which is not specifically defined but created under sections 4A(3) and 4A(5) POCA

Appropriate consent is actual express written consent from GFIU for you (or a person in your firm) to do a prohibited act, and commit one of the principal money laundering offences. It applies in Scenario 1 above.

Deemed consent applies in Scenario 3 above. POCA anticipates that if the GFIU do not respond within 14 working days, transactions should be allowed to proceed.

Negative consent only applies in Scenario 4. The name may be confusing, but it is used to describe another form of deemed consent where POCA anticipates that a transaction should be allowed to proceed where GFIU has refused its consent, but not taken any further action or started a criminal investigation against the suspected criminal.

It is important to note that under sections 4B and 4D POCA the moratorium period described above can be extended by a court order, or by automatic extension, respectively.

It is also important to note that in Scenario 2, you do not have the benefit of any defence and do not have appropriate consent/DAML until Scenario 4 occurs, which means that you should not proceed with the transaction during Scenario 2.

Under section 4B POCA, the Head of the GFIU can apply to the court in order to extend the moratorium period and the court will do so if it is satisfied that all of the following apply:

- an investigation is being carried out in relation to a relevant disclosure (but has not been completed)
- the investigation is being conducted diligently and expeditiously
- further time is needed for conducting the investigation
- it is reasonable in all the circumstances for the moratorium period to be extended

Again, it is vital that you do not proceed with a prohibited act if the moratorium period has been extended by the court, as you will not have the benefit of a defence and do not have appropriate consent/DAML.

Sections 4C and 4D deal with (amongst other matters such as exclusion of persons from any hearing etc.) automatic extension of the moratorium period and further extensions which are for a maximum of 60 working days per extension (starting with the after the day on which the period would otherwise end in accordance with section 4B (4) POCA). It is important to familiarise yourself with how the appeal process works, and how persons and/or information may be excluded from the hearing, but crucial is the understanding that no defence is available during such time as a moratorium period is in place, which means it will become

increasingly difficult to deal with any queries from the suspected person. You must remember your duty to the court and your duty to your client, and reconcile any conflicts that may arise in accordance with applicable codes of conduct.

5.5.1.2 authorised disclosures

In order to benefit from consent/DAML, the disclosure made must be an "authorised disclosure" in accordance with section 4G POCA. To be an authorised disclosure, it must first be made to the GFIU a police officer, a customs officer or a nominated officer by the alleged offender that property is criminal property. Disclosures made to anyone else will not be covered.

Secondly, one of the following three conditions must be satisfied:

- Disclosure is made before you do the prohibited act
- Disclosure is made while the you are doing the prohibited act, but when you began doing the act, you did not know or suspect that the property constituted or represented a person's benefit from criminal conduct, provided that the disclosure is made on your own initiative (and not prompted by GFIU) as soon as it is practicable after you first know or suspect that the property constitutes or represents a person's benefit from criminal conduct
- Disclosure is made after you have done the prohibited act, but you have a reasonable excuse for failing to make the disclosure before you did the prohibited act, provided that the that the disclosure is made on your own initiative (and not prompted by GFIU) as soon as it is practicable for you to make it

If you make a disclosure to the GFIU after you have acted in contravention of section 2 POCA but the disclosure was made on your own initiative as soon as it is reasonable, you will not have committed an offence under that section.

For further information on how to make a disclosure to the GFIU and the process by which consent is gained, see chapter 8 of these Guidance Notes.

5.5.1.3 Reasonable excuse defence

This defence applies to an offence under sections 2, 3 or 4 POCA where a person intended to make a disclosure before doing a prohibited act, but had a reasonable excuse for not disclosing.

Reasonable excuse has not been defined by the courts, but the scope of the reasonable excuse defence is important for legal professional privilege.

It has already been highlighted above that you will have a defence against any of the offences under sections 2, 3 or 4 POCA if you make a disclosure to the GFIU. Where your firm has an appropriate person, you should make your disclosure to the appropriate person. The appropriate person will consider your disclosure and decide whether to make an external disclosure to the GFIU. If your firm does not have an appropriate person, you should make your disclosure directly to the GFIU.

However, you are prevented from disclosing if your knowledge or suspicion is based on privileged information and legal professional privilege is not excluded by the crime/fraud exception[4]. You will have a reasonable excuse for not making an authorised disclosure and will not commit a money laundering offence.

There may be other circumstances which would provide a reasonable excuse; however, these are likely to be narrow. You should clearly document the reason for not making a disclosure on this ground.

[4] Section 5(4) of POCA.

Albeit extreme, one example of reasonable excuse is if you are threatened by a criminal who suspects that you are going to make a disclosure about them and that criminal forces or coerces you to do a prohibited act.

5.5.1.3 official function defence

This defence is not available to relevant financial businesses. It is a defence properly reserved for persons in law enforcement (such as the GFIU for example). The defence states that if the act done in contravention of section 2 POCA (i.e. becoming concerned in an arrangement) is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct

5.5.3 Specific Defences to the principal money laundering offences

5.5.3.1 No knowledge concerned in arrangement

Although difficult to prove, there is a defence of lack of knowledge which applies to the principal offence in section 2(1) POCA. It applies if:

- that you did not know or suspect that the arrangement related to any person's proceeds of criminal conduct; or
- that you did not know or suspect that by the arrangement, the retention or control by or on behalf of A of any property was facilitated or, as the case may be, that by the arrangement any property was used, as mentioned in section 2(1) POCA

5.5.3.2 Adequate consideration defence

This defence applies only as a defence to the offence in section 3(1) POCA if there was adequate consideration for acquiring, using and possessing the criminal property, unless you know or suspect that those goods or services may help another to carry out criminal conduct.

In England the Crown Prosecution Service guidance for prosecutors says the defence applies where professional advisors, such as lawyers or accountants, receive money for or on account of costs, whether from the client or from another person on the client's behalf. Disbursements are also covered. The fees charged must be reasonable, and the defence is not available if the value of the work is significantly less than the money received.

The transfer of funds from client to office account, or vice versa, is covered by the defence.

Returning the balance of an account to a client may be a money laundering offence if you know or suspect the money is criminal property. In that case, you must make an authorised disclosure and obtain consent to deal with the money before you transfer it.

Reaching a matrimonial settlement or an agreement on a retiring partner's interest in a business does not constitute adequate consideration for receipt of criminal property, as in both cases the parties would only be entitled to a share of the legitimately acquired assets of the marriage or the business. This is particularly important where your client would be receiving the property as part of a settlement which would be exempted from section 2(1) POCA due to the case of *Bowman v Fels* (cited above).

The defence is more likely to cover situations where:

- a third party seeks to enforce an arm's length debt and, unknown to them, is given criminal property in payment for that debt
- a person provides goods or services as part of a legitimate arm's length transaction but unknown to them is paid from a bank account which contains the proceeds of crime

5.6 Failure to disclose offences – money laundering

5.6.1 Section 6B POCA – Failure to Disclose: relevant financial business

A person within a relevant financial business commits an offence under section 6B POCA where that person:

- knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering, or is attempting to launder money;
- the information or other matter, on which that knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment; and
- he does not disclose the information or other matter to the GFIU as soon as is reasonably practicable after it comes to his attention.

Therefore, provided these conditions are satisfied you will be under an obligation to disclose such information or matters to the GFIU.

The appropriate person in a relevant financial business will also commit an offence under this section if they do not comply with section 26(2) POCA following any disclosures he receives under section 28 POCA.

In this section, the words ‘knows’ and ‘suspects’ refer to actual knowledge or suspicion - a subjective test. However, independent legal professionals and nominated officers in the regulated sector will also commit an offence if they fail to report when they have ‘reasonable grounds’ for knowledge or suspicion - an objective test. On this basis, they may be guilty of the offence under section 6B POCA if they should have known or suspected money laundering.

For the avoidance of doubt all relevant financial business, including for the purposes of these Guidance Notes the legal profession, is subject to a higher standard and is expected to be more aware and more alert to possible money laundering.

For all failure to disclose offences you must either:

- know the identity of the money launderer or the whereabouts of the laundered property; or
- believe the information on which your suspicion was based may assist in identifying the money launderer or the whereabouts of the laundered property

Our view is that delays in disclosure arising from taking legal advice or seeking help may be acceptable provided you act promptly to seek advice.

5.6.2 Exceptions to failure to disclose offence

There are three situations in which you have not committed an offence for failing to disclose:

- you have a reasonable excuse;
- you are a professional legal adviser or a relevant professional adviser and the information came to you in privileged circumstances.

The first defence is the only one that applies to all three failures to disclose offences; the other two defences are only specifically provided for persons in the regulated sector who are not nominated officers.

5.6.2.1 Reasonable excuse

No offence is committed if there is a reasonable excuse for not making a disclosure, but there is no judicial guidance on what might constitute a reasonable excuse.

However, you are prevented from disclosing if your knowledge or suspicion is based on privileged information and legal professional privilege is not excluded by the crime/fraud exception. It is the Registrar's view that if legal professional privilege applies, you will have a reasonable excuse for not making an authorised disclosure and will not commit a money laundering offence.

There may be other circumstances which would provide a reasonable excuse. For example:

- if it is clear that a regulator or enforcement authority (in Gibraltar or elsewhere) is already aware of the suspected criminal conduct or money laundering and the reporter does not have any additional information which might assist the regulator or enforcement authority, or
- if the only information that a reporter would be providing for the purposes of an authorised disclosure or a report under section 6B POCA is information entirely within the public domain.

This is not intended to be an exhaustive list. Moreover, lawyers should be aware that it will ultimately be for a court to decide if a lawyer's excuse for not making an authorised disclosure report under section 6B was a reasonable excuse. Relevant financial businesses should clearly document their reasons for concluding that they have a reasonable excuse in any given case and, if in doubt, may wish to seek independent legal advice.

5.6.2.2 Ascertaining legal position and privileged circumstances

A person will not be guilty of certain offences under POCA where that person is a notary, independent legal professional, auditor, external accountant or tax advisor and the information has been obtained or received from one of their clients:

- in the course of 'ascertaining the legal position' for their client;
- or whilst performing the task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings.

This defence is known as the ascertaining legal position defence and applies in limited circumstances as follows:

- tipping-off offence under section 5(1) POCA (see chapter 5.7)
- failure to disclose: relevant financial business offence under section 6B(1) POCA (see chapter 5.6)
- requirement to cease transactions under section 15 POCA (see chapter 4.3.5)

This exception does not apply to transactional work, so take a cautious approach to the distinction between advice and litigation work, and transactional work.

Additionally, no offence is committed if the information or other matter giving rise to suspicion comes to a professional legal adviser or relevant professional advisor in 'privileged circumstances'.

You should note that receipt of information in privileged circumstances is not the same as legal professional privilege. It is a creation of POCA designed to comply with the exemptions from reporting set out in the European directives.

Privileged circumstances is not a defined term in POCA but means information communicated:

- by a client, or a representative of a client, in connection with the giving of legal advice to the client, or

- by a client, or by a representative of a client, seeking legal advice from you; or
- by a person in connection with legal proceedings or contemplated legal proceedings.

The exemption will not apply if information is communicated or given to the legal professional with the intention of furthering a criminal purpose (sections 5(4) and 148(5) POCA).

There are overlaps between ascertaining the legal position and privileged circumstances, and it is understood that this may cause confusion. The common feature is that there must be some nexus to legal proceedings.

The UK's Crown Prosecution Service guidance[5] for prosecutors indicates that if a legal professional forms a genuine, but mistaken, belief that the privileged circumstances exemption applies (for example, the client misleads the legal professional and uses the advice received for a criminal purpose) the legal professional will be able to rely on the reasonable excuse defence.

For a further discussion of privileged circumstances see Chapter 6.

5.7 Tipping-off

The offence of tipping-off for money laundering is contained in POCA.

5.7.1 Offences

5.7.1.1 Tipping-off

There is one tipping-off offence which is found in section 5 POCA. You will commit an offence under section 5 POCA where you disclose certain matters which came to you in the course of a business or activity in a relevant financial business. Where you disclose that:

- You or another person has made a disclosure relating to one of the principal money laundering offences to a police officer, customs officer, an appropriate person within your firm or to the GFIU of information that came to you in the course of a relevant financial business; or
- an investigation into allegations of a money laundering offence has been committed, is being contemplated or is being carried out.

5.7.1.2 Prejudicing an investigation

Section 148 POCA contains an offence to prejudice a confiscation, civil recovery, detained cash or money laundering investigation, if the person making the disclosure knows or suspects that an investigation is being, or is about to be conducted.

You only commit this offence if you knew or suspected that the disclosure would, or would be likely to prejudice any investigation.

5.7.2 Defences

5.7.2.1 Section 5 – Tipping-off

Under section 5(3) POCA it will not be an offence under section 5 POCA for a notary, independent legal professional, auditor, external accountant or tax advisor to disclose any information or other matter:

- to a client or his representative in connection with the giving of advice in connection with ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning, judicial

[5] (http://www.cps.gov.uk/legal/p_to_r/proceeds_of_crime_money_laundering/)

proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings; or

- to any person, in contemplation of, or in connection with, ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning, judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before during or after such proceedings

under section 5(6) POCA an auditor, external accountant, tax advisor, notary or independent legal professional will not be liable under this section if they make a disclosure:

- to another such person
- both parties perform their professional activities in an EEA state or territory or in a country or territory which imposes requirements that are equivalent to the Money Laundering Directive; and
- both parties are in different undertakings that share common ownership, management or control.

under section 5(5) POCA it will also not be an offence if disclosure is made by a credit or financial institution belonging to the same a corporate group and:

- disclosure is made to an institution subject to the requirements of the Money Laundering Directive; or
- disclosure is made to an institution in a State or Territory other than an EEA State or Territory which imposed requirements equivalent to those in the Money Laundering Directive and is supervised for compliance of those requirements.

under section 5(7) POCA it will not be an offence to disclose information when this is done for the purposes of preventing money laundering and the following conditions are satisfied:

- the disclosure is between an auditor, external accountant, tax advisor, notary or independent legal professional and another person from the same professional category;
- the person to whom the disclosure is made is situated within the EEA or if outside the EEA, in a State or Territory which imposes requirements that are equivalent to the Money Laundering Directive,
- the disclosure relates to the same customer and the same transaction; and
- the person making the information and the person receiving it are subject to equivalent duties of professional confidentiality and protection of personal data (within the meaning of section 2 of the Data Protection Act 2004).

Finally, under section 5(8) POCA it will not be an offence to make a disclosure to a client where the purpose of that disclosure was to seek to dissuade the client from engaging in criminal activity.

5.7.2.2 Prejudicing an investigation

A person does not commit an offence under section 148 POCA if

- he does not know or suspect that the disclosure is likely to prejudice the investigation,
- the disclosure is made in the exercise of a function under POCA or any other enactment relating to criminal conduct or benefit from criminal conduct or in compliance with a requirement imposed under or by virtue of POCA,
- the disclosure is of a matter within section 5(7) POCA (Tipping-off exemption in order to prevent money laundering) and the information on which the disclosure is based came to the person in the course of a relevant financial business, or

- he is a professional legal adviser and the disclosure is to a client or the client's representative in connection with the giving of advice, or to any person in connection with legal proceedings or contemplated legal proceedings.

5.7.3 Making enquiries of a client

You should make preliminary enquiries of your client, or a third party, to obtain further information to help you to decide whether you have a suspicion. You may also need to raise questions during a retainer to clarify such issues.

There is nothing in POCA which prevents you making normal enquiries about your client's instructions, and the proposed retainer, in order to remove, if possible, any concerns and enable the firm to decide whether to take on or continue the retainer.

These enquiries will only be tipping-off if you disclose that a SAR has been made or that a money laundering investigation is being carried out or contemplated. The offence of tipping-off only applies to a relevant financial business.

It is not tipping-off to include a paragraph about your obligations under the money laundering legislation in your firm's standard client care letter.

Chapter 6 Legal Professional Privilege

6.1 General Comments

Lawyers and notaries are under a duty to keep the affairs of their clients confidential, and the circumstances in which they are able to disclose client communications are strictly limited.

However, sections 2 - 5 of POCA contain provisions for disclosure of information to be made to the GFIU.

Lawyers and notaries also have a duty of full disclosure to their clients. However, section 5 of POCA prohibits disclosure to a client that an investigation is taking place and section148 POCA prohibits disclosure of information in circumstances where it would prejudice an existing or proposed investigation.

Section 152 of POCA deals with Production Orders, 158 with Searches & Warrants and 161 Disclosure.

This chapter examines the tension between a lawyer's duties and this provision of POCA. Similar tensions also arise with respect to the TA 2018 and you may wish to refer to the Law Society's practice note on anti-terrorism in those circumstances available at:

http://www.lawsociety.org.uk/support-services/advice/practice-notes/anti-terrorism/

This chapter should be read in conjunction with chapter 5 of these Guidance Notes and if you are still in doubt as to your position, you should seek independent legal advice.

6.2 Application

This chapter is relevant to any lawyer or notary considering whether to make a disclosure under POCA.

6.3 Duty of confidentiality

A lawyer and a notary is professionally and legally obliged to keep the affairs of clients confidential and to ensure that his staff do likewise. The obligations extend to all matters revealed to a lawyer or to a notary, from whatever source, by a client, or someone acting on the client's behalf.

In exceptional circumstances this general obligation of confidence may be overridden. However, certain communications can never be disclosed unless statute permits this either expressly or by necessary implication. Such communications are those protected by legal professional privilege (“LPP”).

6.4 Legal professional privilege

6.4.1 General overview

LPP is a privilege against disclosure; ensuring clients know that certain documents and information provided to lawyers cannot be disclosed at all. It recognises the client's fundamental human right to be candid with his legal adviser, without fear of later disclosure to his prejudice. It is an absolute right and cannot be overridden by any other interest.

LPP does not extend to everything lawyers have a duty to keep confidential. LPP protects only those confidential communications falling under either of the two heads of privilege – advice privilege or litigation privilege.

For the purposes of LPP, a lawyer only includes lawyers, notaries and their employees and in-house lawyers.

6.4.1 Advice privilege

6.4.1.1 Principle

Communications between a lawyer, acting in his capacity as a lawyer, and a client, are privileged if they are both:

- confidential
- for the purpose of seeking legal advice from a lawyer or providing it to a client

6.4.1.2 Scope

Communications are not privileged merely because a client is speaking or writing to you. The protection applies only to those communications which directly seek or provide advice or which are given in a legal context, that involve the lawyer using his legal skills and which are directly related to the performance of the lawyer's professional duties [Passmore on Privilege 2nd edition 2006].

Case law helps define what advice privilege covers.

6.4.1.3 Communications subject to advice privilege:

- a lawyer's bill of costs and statement of account [*Chant v Brown* (1852) 9 Hare 790]
- information imparted by prospective clients in advance of a retainer will attract LPP if the communications were made for the purpose of indicating the advice required [*Minster v Priest* [1930] AC 558 per Lord Atkin at 584].

6.4.1.4 Communications not subject to advice privilege:

- notes of open court proceedings [*Parry v News Group Newspapers* (1990) 140 New Law Journal 1719] are not privileged, as the content of the communication is not confidential.
- conversations, correspondence or meetings with opposing lawyers [*Parry v News Group Newspapers* (1990) 140 New Law Journal 1719] are not privileged, as the content of the communication is not confidential.
- a client account ledger maintained in relation to the client's money [*Nationwide Building Society v Various Lawyers* [1999] P.N.L.R. 53.]
- an appointments diary or time record on an attendance note, time sheet or fee record relating to a client [*R v Manchester Crown Court, ex p. Rogers* [1999] 1 W.L.R. 832]
- conveyancing documents are not communication so not subject to advice privilege [*R v Inner London Crown Court ex p. Baines & Baines* [1988] QB 579]

6.4.1.5 Advice within a transaction

All communications between a lawyer and his client relating to a transaction in which the lawyer has been instructed for the purpose of obtaining legal advice are covered by advice privilege, notwithstanding that they do not contain advice on matters of law and construction, provided that they are directly related to the performance by the lawyer of his professional duty as legal adviser of his client. [*Three Rivers District Council and others v the Bank of England* [2004] UKHL 48 at 111]

This will mean that where you are providing legal advice in a transactional matter (such as a conveyance) the advice privilege will cover all:

- communications with,
- instructions from, and

- advice given to

the client, including any working papers and drafts prepared, as long as they are directly related to your performance of your professional duties as a legal adviser.

6.4.2 Litigation privilege

6.4.2.1 Principle

This privilege, which is wider than advice privilege, protects confidential communications made after litigation has started, or is reasonably in prospect, between either:

- a lawyer and a client
- a lawyer and an agent, whether or not that agent is a lawyer
- a lawyer and a third party

These communications must be for the sole or dominant purpose of litigation, either:

- for seeking or giving advice in relation to it
- for obtaining evidence to be used in it
- for obtaining information leading to obtaining such evidence

6.4.3 Important points to consider

An original document not brought into existence for these privileged purposes and so not already privileged, does not become privileged merely by being given to a lawyer for advice or other privileged purpose.

Further, where you have a corporate client, communication between you and the employees of a corporate client may not be protected by LPP if the employee cannot be considered to be 'the client' for the purposes of the retainer. As such, some employees will be clients, while others will not. [*Three Rivers District Council v the Governor and Company of the Bank of England* (no 5) [2003] QB 1556]

It is not a breach of LPP to discuss a matter with your nominated officer for the purposes of receiving advice on whether to make a disclosure.

6.4.4 Crime/fraud exception

LPP protects advice you give to a client on avoiding committing a crime [*Bullivant v Att-Gen of Victoria* [1901] AC 196] or warning them that proposed actions could attract prosecution [*Butler v Board of Trade* [1971] Ch 680]. LPP does not extend to documents which themselves form part of a criminal or fraudulent act, or communications which take place in order to obtain advice with the intention of carrying out an offence [*R v Cox & Railton* (1884) 14 QBD 153]. It is irrelevant whether or not you are aware that you are being used for that purpose [*Banque Keyser Ullman v Skandia* [1986] 1 Lloyds Rep 336].

6.4.4.1 Intention of furthering a criminal purpose

It is not just your client's intention which is relevant for the purpose of ascertaining whether information was communicated for the furtherance of a criminal purpose. It is also sufficient that a third party intends the lawyer/client communication to be made with that purpose (e.g. where the innocent client is being used by a third party) [*R v Central Criminal Court ex p Francis & Francis* [1989] 1 AC 346].

6.4.4.2 Knowing a transaction constitutes an offence

If you know the transaction you're working on is a principal offence, you risk committing an offence yourself. In these circumstances, communications relating to such a transaction are not privileged and should be disclosed.

6.4.4.3 Suspecting a transaction constitutes an offence

If you merely suspect a transaction might constitute a money laundering offence, the position is more complex. If the suspicions are correct, communications with the client are not privileged. If the suspicions are unfounded, the communications should remain privileged and are therefore non-disclosable.

6.4.4.4 Prima facie evidence

If you suspect you are unwittingly being involved by your client in a fraud, the courts require prima facie evidence before LPP can be displaced [*O'Rourke v Darbishire* [1920] AC 581]. The sufficiency of that evidence depends on the circumstances: it is easier to infer a prima facie case where there is substantial material available to support an inference of fraud. While you may decide yourself if prima facie evidence exists, you may also ask the court for directions [*Finers v Miro* [1991] 1 W.L.R. 35].

In England, the Crown Prosecution Service guidance[6] for prosecutors indicates that if a lawyer forms a genuine, but mistaken, belief that the privileged circumstances exemption (see 6.5 below) applies (for example, the client misleads the lawyer and uses the advice received for a criminal purpose) the lawyer will be able to rely on the reasonable excuse defence. It is likely that a similar approach would be taken with respect to a genuine, but mistaken, belief that LPP applies.

You should not make a disclosure unless you know of prima facie evidence that you are being used in the furtherance of a crime.

6.5 Privileged circumstances

Although the wording is not exactly the same in all these sections, the essential elements of the exemption are:

(a) that person is a notary or an independent legal professional, and

(b) the information has been obtained on or received from one of their clients-

  (i) in the course of ascertaining the legal position for their client; or

  (ii) whilst performing the task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings,

The defence covers notaries, independent legal professionals, auditor, external accountant or tax advisor.

6.6 Differences between privileged circumstances and LPP

6.6.1 Protection of advice

When advice is given or received in circumstances where litigation is neither contemplated nor reasonably in prospect, except in very limited circumstances communications between you and third parties will not be protected under the advice arm of LPP.

Privileged circumstances, however, exempt communications regarding information communicated by representatives of a client, where it is in connection with your giving legal advice to the client, or the client seeking legal advice from you. This may include communications with:

- a junior employee of a client (if it is reasonable in the circumstances to consider them to be a representative of the client)

[6] (http://www.cps.gov.uk/legal/p_to_r/proceeds_of_crime_money_laundering/)

- other professionals who are providing information to you on behalf of the client as part of the transaction

You should consider the facts of each case when deciding whether or not a person is a representative for the purposes of privileged circumstances.

6.6.2 Losing protection by dissemination

There may be circumstances in which a legal adviser has communicated to him information which is subject to legal professional privilege, but which does not fall within the definition of privileged circumstances.

For example, a lawyer representing client A may hold or have had communicated to him information which is privileged as between client B and his own lawyer, in circumstances where client A and client B are parties to a transaction, or have some other shared interest.

The sharing of this information may not result in client B's privilege being lost, if it is stipulated that privilege is not waived (Gotha City v Sotheby's (no1) [1998] 1 WLR 114).

However, privileged circumstances will not apply because the information was not communicated to client A's lawyer by a client of his in connection with the giving by him of legal advice to that client. However, if it was given to him by any person in connection with legal proceedings or contemplated legal proceedings, privileged circumstances would apply.

In such circumstances, the lawyer representing client A would not be able to rely on privileged circumstances, but the information might still be subject to LPP, unless the crime/fraud exemption applied.

6.7 When do I disclose?

If the communication is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under POCA.

If the crime/fraud exception does apply, the communication will still be confidential. However, the material is disclosable under POCA and can be disclosed.

6.8 Protected disclosures

Section 4H POCA, enacted in 2017 creates a new category of disclosure known as protected disclosures, which essentially allows a person to make a disclosure to the GFIU, a police officer, a customs officer or a nominated officer without breaching any restriction on the disclosure of information (however imposed).

The following three conditions must be satisfied

- firstly, that the information or other matter disclosed came to the person making the disclosure (the discloser) in the course of his trade, profession, business or employment
- secondly, that the information or other matters causes the discloser to know or suspect, or have reasonable grounds for knowing or suspecting that another person is engaged in money laundering
- thirdly, that the disclosure is made to the GFIU, a police officer , a customs officer or a nominated officer as soon as is practicable after the information or other matter comes to the discloser

Additionally, if made to a nominated officer, the disclosure must be made during the course of the discloser’s employment.

The disclosure must consist of either or both of:

- the identity of another person is whom the discloser knows or suspects, or has reasonable grounds for knowing or suspecting, that such other person is engaged in money laundering
- the whereabouts of property forming the subject-matter of the money laundering that the discloser knows or suspects, or has reasonable grounds for knowing or suspecting, that other person to be engaged in

Chapter 7 Terrorist Property Offences

7.1 General Comments

Terrorist organisations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies. The TA 2018 criminalises not only the participation in terrorist activities but also the provision of monetary support for terrorist purposes.

7.2 Application

All persons are required to comply with the TA 2018, The principal terrorist property offences in sections 5 TA 2018 apply to all persons and therefore to all lawyers and notaries. However, section 40 and 46 contain exceptions from the disclosure obligations for certain professionals such as independent legal professionals, auditors and tax advisors.

7.3 Principal terrorist property offences

7.3.1 Section 35 TA 2018 – fundraising

It is an offence to be involved in fundraising if you have knowledge or reasonable cause to suspect that the money or other property raised may be used for terrorist purposes. You can commit the offence by:

- inviting others to make contributions
- receiving contributions
- making contributions towards terrorist funding, including making gifts and loans.

In section 35 TA 2018, 'contributions' is to be construed as including money or other property and it is no defence that the money or other property is a payment for goods and services.

7.3.2 Section 36 TA 2018 – use or possession

It is an offence to use or possess money or other property for terrorist purposes, including when you have reasonable cause to suspect they may be used for these purposes.

7.3.3 Section 37 TA 2018 – arrangements

It is an offence to become involved in an arrangement which makes money or other property available to another if you know, or have reasonable cause to suspect it may be used for terrorist purposes.

7.3.4 Section 39 TA 2018 – retention or control (money laundering)

It is an offence to enter into or become concerned in an arrangement facilitating the retention or control of terrorist property by, or on behalf of, another person including, but not limited to the following ways:

- by concealment
- by removal from the jurisdiction
- by transfer to nominees

It is a defence if you did not know, and had no reasonable cause to suspect, that the arrangement related to terrorist property.

Read about arrangements under POCA in chapter 5

7.4 Defences to principal terrorist property offences

There are a number of defences to the main offences in sections 5 – 8 TA 2018. These defences are mostly contained in section 9 TA 2018.

You will not commit an offence under any of the above sections if you are acting with the express consent of the GFIU in the following circumstances:

- if you disclose to the GFIU:
- your suspicion or belief that the money or other property is terrorist property; and
- the information on which your suspicion or belief is based
- your disclosure is made:
- after you become involved in the transaction or arrangement;
- on your own initiative; and
- as soon as is reasonably practicable
- you did not continue to be involved in the transaction or arrangement after the GFIU forbid you from doing so.

The defence of disclosure to the GFIU is also available to an employee who makes a disclosure about terrorist property offences in accordance with the internal reporting procedures laid down by the firm.

Read chapter 8 of these Guidance Notes for more information on how to make a disclosure and gaining consent.

It is also a defence for a person charged with an offence under sections 5(2) and (3) and 6-8 of TA 2018 to prove that they intended to make a disclosure but have a reasonable excuse for failing to do so. See 5.7.1 of these Guidance Notes.

Additionally, if you are charged for an offence under section 8 TA 2018 it will be a defence to prove that you did not know and had no reasonable cause to suspect that the arrangement related to terrorist property

Importantly, section 46 95) TA 2018 provides that you will not be required to make a disclosure to the GFIU under section 9 TA 2018 if:

- he has a reasonable excuse for not disclosing the information or other matter;
- he is a professional legal adviser or relevant professional adviser and the information or other matter came to him in privileged circumstances;
- subsection (6) applies to him, i.e. if-
- the person is employed by, or is in partnership with, a professional legal adviser or relevant professional adviser to provide the adviser with assistance or support;
- the information or other matter comes to the person in connection with the provision of such assistance or support; and the information or other matter came to the adviser in privileged circumstances

Making enquiries of a client

You will often make preliminary enquiries of your client, or a third party, to obtain further information to help you to decide whether you have a suspicion. You may also need to raise questions during a retainer to clarify such issues.

7.6 Other terrorist property offences in statutory instruments

7.6.1 The offences

Under the UK Statutory Instrument entitled the Al Qaida and Taliban (United Nations Measures) (Overseas Territories) Order 2002 you must not:

- deal with the funds or economic resources of designated persons
- make funds and economic resources available, directly or indirectly for the benefit of designated persons.

Under the UK Statutory Instrument entitled the Terrorism (United Nations Measures) (Overseas Territories) Order 2001, you must not:

- invite another person to provide funds;
- receive funds from another person; or
- provide funds to another person

directly intending that they should be used, or knowing that they may be used, for the purposes of terrorism.

Finally, you must not knowingly and intentionally participate in activities that would directly or indirectly circumvent the financial restrictions, enable, or facilitate the commission of any of the above offences.

It is a defence if you did not know nor had no reason to suspect that you were undertaking a prohibited act with respect to a designated person.

In relation to funds, ‘deal with’ is defined by the legislation as:

- using, altering, moving, allowing access to or transferring
- dealing with in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination, or
- making any other change that would enable use, including portfolio management.

In relation to economic resources, 'deal with' is defined as:

- using to obtain funds, goods, or services in any way, including (but not limited to) by selling, hiring or mortgaging the resources.

Financial services are defined broadly and include advisory services such as providing advice on

- acquisitions
- corporate restructuring and strategy.

7.6.2 Obtaining permission from the GFIU

Under section 9 TA 2018 you must not proceed with a transaction without permission from the GFIU where a client or the intended recipient of funds from the transaction is identified as a designated person.

You must do all of the following:

- suspend the transaction pending advice from the GFIU
- contact the GFIU to seek permission to deal with the funds
- consider whether you have a suspicion of money laundering or terrorist financing which requires a report to the GFIU You must not:
- return funds to the designated person without the approval of the GFIU

The GFIU has the power to exempt certain transactions from the financial restrictions. Requests are considered on a case-by-case basis, to ensure that there is no risk of funds being diverted to terrorism.

Contact the GFIU to request such permission or obtain advice regarding financial restrictions at:

The Gibraltar Financial Intelligence Unit (GFIU)
Address: Suite 945, Europort, Gibraltar
Telephone: +350 200 70211
Fax: +350 200 70233
E-Mail: admin@gfiu.gov.gi

Chapter 8 Making a Disclosure

8.1 General Comments

The disclosure regime for money laundering and terrorist financing is run by the GFIU. The

GFIU was established under the umbrella of the Gibraltar Co-ordinating Centre for Criminal

Intelligence and Drugs. It is staffed by officers seconded from HM Customs Gibraltar and The Royal Gibraltar Police and is a member of the Egmont Group of Financial Intelligence Units. The GFIU is manned from 0900hrs to 1700hrs Mondays to Fridays.

In 2017 a whole new Part was inserted into POCA (Part IA) dealing with the establishment and functioning of GFIU as well as providing them it with new powers.

The GFIUs functions are;

- To gather, store, analyse and disseminate intelligence
- To act as the recipient for STRs
- To exchange information regarding criminal conduct
- To consent or deny consent to STRs

8.2 Format of report

The use of a standard format for the reporting of disclosures is important and all firms / sole practitioners are encouraged to register to use the GFIU's online reporting system (Themis).

Access to this system can be obtained from the GFIU https://www.gfiu.gov.gi/reporting.

Further information and advice on Themis can be obtained from GFIU.

Sufficient information should be disclosed on the suspicious transaction, including the reason for the suspicion, to enable the investigating officer to conduct appropriate enquiries.

The suspected criminality should be stated so that the report may be passed to the appropriate investigation team with the minimum of delay.

Where additional relevant evidence is held which could be made available to the investigating officer, this should be added to the disclosure. Themis allows for the disclosure of additional information in various formats

The receipt of all disclosures will be acknowledged by GFIU. In the majority of cases, written consent will also be given to continue processing the transaction. However, in exceptional circumstances such as the imminent arrest of a customer and restraint of assets, consent may not be given.

The reporting firm / sole practitioner concerned will be made aware of the situation and should follow the directions of the Police or Customs officer in charge of the investigation.

Where a firm / sole practitioner has submitted a suspicious transaction report to GFIU or where it knows that a client or transaction is under investigation, it should not destroy any relevant records without the agreement of the authorities even though the five-year limit may have been reached.

8.3 After a report has been submitted

Following receipt of a disclosure and initial research within GFIU, the information contained in the disclosure (not the disclosure itself) is allocated to a designated, trained financial investigator in the Royal Gibraltar Police or HM Customs, Gibraltar. An investigation will be mounted if appropriate, which will seek to obtain admissible evidence of criminal activity, leading ultimately to prosecution. As the investigation proceeds, evidential material may also be sought from the institution which made the original disclosure, generally by way of a Court Order. Where appropriate, information contained in the disclosure may also be copied to designated officers at the relevant regulatory authorities in Gibraltar.

The customer is not approached in the initial stages of the investigation and will not be approached unless criminal activity is identified. Courts generally recognise the need to protect sources of sensitive intelligence, and it is the duty of investigators to seek in such circumstances to obtain the relevant evidence by independent means.

The money laundering and terrorism legislation is drafted in such a way that reports submitted to GFIU may be allocated only to Police or Customs Officers for investigation.

Access to the information contained in disclosures is restricted to designated officers within the Royal Gibraltar Police, HM Customs Gibraltar and other regulatory authorities in Gibraltar. Whilst other officers may be involved in a subsequent investigation, the original information is restricted to GFIU and these designated officers. Maintaining the integrity of the confidential relationship which has developed between law enforcement agencies and disclosing institutions is of paramount importance.

It is therefore important that all disclosures are made to GFIU in accordance with these procedures. It is recognised however that there may be occasions when an urgent operational response is required which can only be effected by direct contact with RGP or Customs. In such circumstances, the GFIU must be advised as soon as practicable and a written disclosure submitted as usual.

Whilst the legislation permits disclosure to any Police or Customs Officer only GFIU will issue letters of acknowledgement and consent.

Following the submission of a disclosure report, a firm is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal commercial reasons. It must not alert the customer to the fact of the disclosure as to do so would constitute a “tipping-off” offence. Close liaison with GFIU and the investigating officer is encouraged in such circumstances so that the interests of all parties may be fully considered.

8.3.1 Feedback from the Investigating Authorities

The provision of feedback by the investigating agency to the disclosing firm is recognised as an important element of the system. Case officers in charge of investigations are encouraged to provide feedback, in general terms, as to the progress of investigations. GFIU may also provide feedback on such cases, and will provide to the institutions on a regular basis, feedback as to the volume and quality of disclosures and on the levels of successful investigations arising from them. Such information, whether provided verbally or in written form should not be used as the basis of subsequent commercial decisions.

Firms should ensure that all contact between particular sections of their organisation and law enforcement agencies is reported back to the Money Laundering Reporting Officer, so that an informed overview of the situation may be obtained. The MLRO should ensure that there is an established close co-operation and liaison with GFIU. In addition, Police or Customs will continue to provide information on request to a disclosing firm in order to establish the current status of a specific investigation.

Disclosing firms should not be disheartened by a perceived lack of an immediate result following a disclosure, and should guard against dismissing further suspicions based on similar circumstances. Criminal investigations can, by their very nature, take weeks, months or even years to result in arrest and conviction.

A disclosure may be the very first piece in a complex puzzle, or it may be the final piece which completes the picture.

8.4 Suspected Terrorists or Terrorist Financing Activities - additional requirements

The Terrorism Act provides for four different types of terrorist financing offences:

- Raising funds for terrorism (s5).
- Use of and possession of money and other property for terrorism (s6).
- Arranging funds for terrorism (s7).
- Arrangements for retention or control of terrorist property (s8).

Under the legislation the only time a person is allowed to take part in any of the above is with the express consent of a Police officer so it would therefore follow that having a suspicion or belief that any of the above is taking place imposes an obligation on a person to stop the transaction or activity.

Where a firm has a suspicion or belief that terrorist financing is taking place it must ensure that the transaction or activity does not proceed any further until a disclosure to GFIU has been made and consent for the transaction or activity to proceed has been given.

A disclosure made under the Terrorism Act must be accompanied with the information on which the suspicion or belief is based and must be made as soon as is practicable after the suspicion or belief was raised.

Two other items of legislation which are applicable in Gibraltar are the Terrorism (United Nations Measures) (Overseas Measures) Order 2001 and The Al-Qaeda and Taliban (United Nations Measures) (Overseas Territories) Order 2002 (the “Terrorism Orders”). These Orders make provisions for the freezing and reporting of accounts held with financial institutions of named individuals.

Firms are required, in order to comply with the provisions of the Terrorism Orders to search their customer base to ascertain whether any individuals named in them are positively matched. If a positive match is discovered, firms are required to freeze these business relationships and report this to the Governor.

8.5 Data subjects, access rights, suspicious transaction reports and the Data Protection Act

Occasionally, a request for access to personal data held by a data controller (a firm) under Section 14 of the DPA will include within its scope one or more money laundering/terrorist financing suspicious transaction reports which have been submitted in relation to that customer to GFIU. Although it might be instinctively assumed that to avoid tipping off there can be no question of ever including this information when responding to the customer, an automatic assumption to that effect must not be made, even though in practice it will only rarely be decided that it is appropriate to include it.

On making a request in writing to a data controller an individual is normally entitled to have made available to him in an intelligible form all the information that constitutes his personal data and any information available to the data controller as to the source of that data.

Section 19 of the Data Protection Act provides that personal data is exempt from disclosure under Section 14 of the Act in any case where the application of that provision would be

likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. However, even when relying on an exemption, data controllers (i.e. firms) should provide as much information as they can in response to a request.

Likewise, section 34A(5) POCA makes it clear that a data subject's right of access to personal data relating to him shall be lawfully partially or fully restricted where such partial or complete restriction is necessary and proportionate to- (a) enable the relevant financial business or supervisory body to fulfil its tasks properly for the purposes of POCA or the 4MLD; or (b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of POCA or the 4MLD and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.

Chapter 9 Enforcement

9.1 General comments

Gibraltar's AML/CTF regime is one of the most robust in Europe. Breaches of obligations under the regime are backed by disciplinary and criminal penalties.

Law enforcement agencies and regulators are working co-operatively with the regulated sector specifically and lawyers and notaries generally to assist compliance and increase understanding of how to effectively mitigate risks. However, be in no doubt of the seriousness of the sanctions for a failure to comply, nor the willingness of supervisory and enforcement bodies to take appropriate action against non-compliance.

9.2 Supervision under POCA

Section 29 POCA provides for several bodies to be Supervisory Authorities for different parts of the regulated sector.

Where a person in a relevant financial business is covered by more than one Supervisory Authority, either the joint Supervisory Authorities must negotiate who is to be the sole supervisor of the person, or they must co-operate in the performance of their supervisory duties.

A Supervisory Authority must:

- monitor effectively the persons it is responsible for
- take necessary measures to ensure their compliance with the requirements of the POCA
- report to the GFIU any suspicion that a person it is responsible for has engaged in money laundering or terrorist financing

The Minister may by order published in the Gazette add to, delete from, or amend the list of Supervisory Authorities in Part I of Schedule 2 of POCA.

9.2.1 Lawyers Regulation for AML/CFT Compliance

Under Part I of Schedule 2 of POCA, the Registrar of the Supreme Court has been appointed as a Supervisory Authority by the Minister for Finance by notice in the Gazette for the purposes of monitoring compliance by the legal profession for AML/CFT Systems of Controls.

9.3 Offences and penalties

Not complying with AML/CTF obligations puts you at risk of committing criminal offences. Below is a summary of the offences and the relevant penalties. In addition to the principal offences, you could also be charged with offences of conspiracy, attempt, counselling, aiding, abetting or procuring a principal offence, depending on the circumstances.

9.3.1 POCA

Section	*Description*	*Penalty*
2(1)	Arrangements regarding criminal property	On summary conviction up to six months imprisonment or a fine (not exceeding level 5 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both
6B(1)	Failure to disclose offence	On summary conviction up to six months imprisonment or a fine (not exceeding level 5 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both
3(1)	Acquires, uses or has possession of criminal property	On summary conviction up to six months imprisonment or a fine (not exceeding level 5 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both
4F	discloses the fact that a suspension order has been issued under section 4F	On summary conviction up to six months imprisonment or a fine (not exceeding level 5 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both
	failure to take action to suspend a transaction following a suspension order made under section 4F	On summary conviction up to six months imprisonment or a fine (not exceeding level 5 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both
4(1)	Conceals or transfers proceeds of criminal property	On summary conviction up to six months imprisonment or a fine (not exceeding level 5 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both
5	Tipping-off	On summary conviction up to six months imprisonment or a fine (not exceeding level 5 on the standard scale) or both On conviction on indictment up to five years imprisonment or a fine (unlimited) or both
148	Prejudicing an investigation	On summary conviction up to six months imprisonment or a fine (not exceeding the statutory maximum) or both On conviction on indictment up to five years imprisonment or a fine (unlimited) or both

Section	*Description*	*Penalty*
163	Failure to comply with disclosure order under section 161 without reasonable excuse	On summary conviction up to six months imprisonment or a fine (not exceeding level 5 on the standard scale) or both
	Knowingly or recklessly making a false or misleading statement further to a disclosure order under section 161	On summary conviction up to six months imprisonment or a fine (not exceeding the statutory maximum) or both On conviction on indictment up to two years imprisonment or a fine (unlimited) or both

Section 170 creates an offence for financial institutions, so is not relevant to lawyers or to notaries.

Section 1DC (1) of Part IA POCA creates an offence for failing to provide GFIU with further information under section 1DA (4) POCA. Section 1DA POCA applies when a report is made to the GFIU (which includes but is not limited to an SAR), and the GFIU considers it necessary to request additional information from any relevant person ("A") who is not the reporter but who– (i) is mentioned in or otherwise identifiable from the report, or (ii) to the reasonable knowledge or belief of the GFIU, holds information that is relevant to analysis of the report. The person guilty of an offence under this section 1DC (1) POCA shall be liable (i) on summary conviction to a term of imprisonment not exceeding 1 year or a fine (not exceeding level 5 on the standard scale) or both; and (ii) on conviction on indictment to a term of imprisonment not exceeding 2 years or a fine (unlimited) or to both

In addition to the above Section 33 lists a number of sections, the breach of which is an offence. The possible penalty is the same for all breaches of the below sections depending on summary conviction or conviction on indictment:

- On summary conviction a fine (not exceeding level 5 on the standard scale)
- On conviction on indictment up to two years imprisonment or a fine (unlimited) or both

Section	**Description**
11(1)	Applying CDD to new customers, occasional transactions amounting to 15,000 euro or more, suspects money laundering or terrorist financing or doubts the veracity or adequacy of documents, data or information previously obtained for purposes of identification or verification
11(2)	Applying CDD to existing customers
11(3)	Determining extent of CDD on a risk- sensitive basis and being able to demonstrate this to the Supervisory Authority
12(1)	Conducting ongoing monitoring
12(3)	Determining the extent of ongoing monitoring on a risk-sensitive basis and being able to demonstrate this to the Supervisory Authority.
13(2)	Verification prior to the establishment of a business relationship or carrying out of an occasional transaction
14	Relates to casinos
15(1) (a)	Not use a bank account without CDD

15(1) (b)	Not establish a business relationship or carry out an occasional transaction if no CDD
15(1) (c)	Terminate existing relationship or occasional transaction if no CDD
15(1) (d)	Consider whether he is required to make a disclosure to the GFIU
17	Conduct enhanced due diligence and ongoing monitoring
21 (1)	financial and credit institutions requiring branches and subsidiary undertakings located in non-EEA State / Territory to apply equivalent CDD measures
21 (2)	financial and credit institutions to inform relevant regulator where non-EEA State/Territory does not allow compliance with 21(1), and take additional measures
22 (1)	credit institutions not to enter into/continue banking relationship with shell banks
22 (2)	credit institutions not to take measures to ensure they do not enter into/continue banking relationship with banks known to permit their accounts to be used by shell banks
22 (3)	credit or financial institution carrying on business in Gibraltar must not set up an anonymous account or an anonymous passbook for any new or existing customer.
22 (4)	establishes meaning of shell bank
25 (1)	Keep your own records
25 (4)	Keep records others have relied on
25 (5)	Be prepared to provide records others have relied on
25 (6)	Ensure those you rely on are willing to provide records
26 (1)	Establish policies and procedures
26 (4)	financial and credit institutions to maintain systems to enable them to respond fully and rapidly to enquiries from the GFIU on nature of their business relationships during the previous five years
26 (5)	financial and credit institutions to be able to communicate where relevant the equivalent policies and procedures required under section 26 that are maintained in its branches and subsidiary undertakings located outside Gibraltar.
27	Train relevant employees
Directions under 24	Not to act where FATF makes a direction

Finally, you should note the table in section 42 POCA, which provides terms of imprisonment for failure to comply with a court order for payment of any amount under section 35 POCA, which deals with confiscation orders.

9.3.2 TA 2018

Section	Description	Penalty
5	Fundraising	On summary conviction up to six months imprisonment or a fine (not exceeding level 4 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both

Section	Description	Penalty
6	Use and possession	On summary conviction up to six months imprisonment or a fine (not exceeding level 4 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both
7	Funding arrangements	On summary conviction up to six months imprisonment or a fine (not exceeding level 4 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both
8	Retention or control	On summary conviction up to six months imprisonment or a fine (not exceeding level 4 on the standard scale) or both On conviction on indictment up to fourteen years imprisonment or a fine (unlimited) or both

The relevant section imposing such penalties is section 54 TA 2018.

9.4 Joint liability

Section 34 POCA provides that offences under POCA can be committed by a firm as a whole, whether it is a body corporate, partnership or unincorporated association.

However, if it can be shown that the offence was committed with the consent, contrivance or neglect of an officer, partner or member, then both the firm and the individual can be liable.

9.5 Prosecution authorities

The Attorney General (via the Office of Criminal Prosecutions and Litigation of the Government Law Offices) is a prosecuting authority for offences under POCA and the TA.

Chapter 10 Civil Liability

10.1 General Comments

POCA aims to deprive wrongdoers of the benefits of crime, not compensate the victims. The civil law provides an opportunity for victims to take action against wrongdoers and those who have assisted them, through a claim for constructive trusteeship. Victims often target the professional adviser in civil claims because they are more likely to be able to pay compensation, often by reason of their professional indemnity cover.

If you believe that you may have acted as a constructive trustee, you should seek legal advice.

10.2 Constructive trusteeship

Constructive trusteeship arises as a result of your interference with trust property or involvement in a breach of fiduciary duty. These are traditionally described respectively as knowing receipt and knowing assistance.

Your liability in either case is personal, an equitable liability to account, not proprietary. A constructive trustee has to restore the value of the property they have received or compensate the claimant for the loss resulting from the assistance with a breach of trust or fiduciary duty. See Lord Millett's judgment in Dubai Aluminium Co Ltd v Salaam [2002] 3 W.L.R 1913, at paragraph 1933.

The state of your knowledge is key to this liability. Records of CDD measures undertaken and disclosures or your notes provide evidence of your knowledge and intentions.

10.3 Knowing receipt

Liability for knowing receipt will exist where a person receives property in circumstances where the property is subject to a trust or fiduciary duty and contrary to that trust applies the property for their use and benefit. Considering each element in turn:

10.3.1 Receipt

- You must have received the property in which the claimant has an equitable proprietary interest.
- The property must be received:
- in breach of trust
- in breach of a fiduciary duty, or
- legitimately, but then misapplied

10.3.2 For your use and benefit

When you receive money, e.g. as an agent, or, as in the case of a lawyer's or notary's client account, as a trustee of a bare trust, then you are not liable for knowing receipt as it is not received for your use or benefit. You may however still be liable for knowing assistance.

Receiving funds that you apply in satisfaction of your fees will however be beneficial receipt and could amount to knowing receipt.

10.3.3 You must be at fault

What constitutes fault here is the subject of some debate. The Court of Appeal in *Bank of Credit and Commerce International (Overseas) Ltd and another v Akindele* [2001] Ch.437 held that the test is whether you acted unconscionably. The test is a subjective one which includes actual knowledge and wilful blindness. The factors the court identified were that:

- You need not have acted dishonestly. It is enough to know a fiduciary or trust duty has been breached.
- Your knowledge of funds' provenance should be such that it was unconscionable for you to retain any benefit.

It is unclear whether a reckless failure to make enquiries a reasonable person would have made would be sufficient to establish liability. In Dubai Aluminium Co Ltd (cited above) Lord Millett described knowing receipt as dishonest assistance. However, that may well have been specific to the particular facts he was considering.

10.4 Knowing assistance

If you help in a breach of fiduciary or trust duties then you are personally liable for the damage and loss caused. See *Twinsectra v Yardley* [2002] 2 W.L.R 802.

The requirements to establish liability of this kind are:

10.4.1 Assistance in a breach of trust or fiduciary duty

The breach need not have been fraudulent, (see Royal Brunei Airlines v Tan [1995] 2 AC 378), and you do not need to know the full details of the trust arrangements you help to breach, nor the obligations incumbent on a trustee/fiduciary.

You assist if you either:

- know that the person you are assisting is not entitled to do the things that they are doing
- have sufficient ground for suspicion of this

10.4.2 You must be at fault

There must be dishonesty, not just knowledge. The test for dishonesty is objective. The Privy Council in *Eurotrust v Barlow Clowes* [2006]1 All ER stated that the test is whether your conduct is dishonest by the standards of reasonable and honest people, taking into account your specific characteristics and context, i.e. your intelligence, knowledge at the relevant time, and your experience.

Conscious impropriety is not required; it is enough to have shown wilful blindness by deliberately failing to make the enquiries that a reasonable and honest person would make.

10.5 Making a disclosure to the GFIU

10.5.1 Risk of defensive disclosure to the GFIU

Where you suspect or know your clients are involving you in circumstances that could amount to one of the principal money laundering offences, you must disclose your suspicions to the GFIU, subject to the constraints of LPP, and obtain their permission before allowing the transaction to proceed.

Consent from the GFIU only protects you from falling foul of the anti-money laundering regime. It will not defend you from civil liability. In fact, obtaining consent may create the very evidence on which a claimant can rely to found a civil liability.

It is therefore vital that you only disclose to the GFIU those situations fulfilling the statutory tests in Part 2 of POCA; knowledge or suspicion of money laundering, or reasonable grounds to suspect money laundering.

10.5.2 While awaiting consent from the GFIU

Your position can be difficult. While the client will be expecting you to implement their instructions, you may be unable to do so, or give explanations, as you may risk a tipping-off offence.

The client may seek a court order for the return of the funds on the basis that you are breaching their retainer.

Case law provides no direct authority on the point, but a ruling on the obligations of banks is helpful in suggesting the courts' likely view of the obligations imposed on lawyers and on notaries. In *K Ltd v National Westminster Bank plc and others* [2006] EWCA Civ 1039 the Court of Appeal ruled that a bank's contract with the customer was suspended whilst the moratorium period was in place, so the customer had no right to an injunction for return of monies. The court also said that as a matter of discretion, the court would not force the bank to commit a crime.

The Court of Appeal also approved the use of a letter to the court from the bank as evidence of its suspicion.

10.5.3 Where the GFIU consents

In continuing with a transaction, you will have to show that either:

- Although you had sufficient suspicion to justify a disclosure to the GFIU, your concerns were not such as to render them accountable on a constructive trustee basis. Courts are likely to take into account the fact that you will generally operate in a relevant financial business, and assume a degree of sophistication as a result of anti-money laundering training. Lawyers and notaries are expected to be able to account for decisions to proceed with transactions.
- Your suspicions were either removed or reduced by subsequent information or investigations.

The Courts have provided limited assistance in this area. In *Bank of Scotland v, A Ltd and others* [2001] 1 W.L.R 751 it was stated that complying with a client's instructions was a commercial risk which a bank had to take. While the court gave some reassurance on the unlikelihood of any finding of dishonesty against an institution that had sought guidance from the court and did not pay funds away, this is of limited assistance because it is for the positive act of paying away funds that protection will be needed.

Such protection is not readily available. In *Amalgamated Metal Trading v City of London Police Financial Investigation Unit and others* [2003] 1 W.L.R 2711 the court held that while a court could make a declaration on whether particular funds were the proceeds of crime, a full hearing would be required with both the potential victim and the client participating. There would have to be proof on the balance of probabilities that the funds were not the proceeds of crime. In practice this is highly unlikely to be practical.

10.6 Notify your professional indemnity insurers

You must notify your insurers at the earliest opportunity of any circumstances that might give rise to a claim. You should consider notifying your insurers whenever you make a disclosure to the GFIU. In particular:

- you may be unable to follow clients' instructions, e.g.:
- where consent has not been given by the GFIU;
- where you judge you may be exposing yourself to a civil claim, so may face a claim from the client for failure to meet the terms of your retainer
- The GFIU has given consent, but where you fear civil liability. Consider whether to not proceed with the transaction.

Any disclosure made to insurers should clearly state any money laundering issues, that a disclosure has been made to the GFIU and, if known, the GFIU's response.

You may be concerned about a tipping-off offence under section 5 POCA when talking to your insurer.

A key element of the offence is the likelihood of prejudicing an investigation. The risk of this is small when disclosing to a reputable insurer. Insurers are also regulated for the purposes of anti-money laundering and subject to the same obligations.

For further advice on tipping-off, see chapters 5, 7 and 8 of these Guidance Notes

For further information about avoiding tipping-off in a particular case, contact the GFIU on +350 200 70211.

Chapter 11 Money Laundering Warning Signs

11.1 General Comments

POCA requires you to conduct ongoing monitoring of your business relationships and take steps to be aware of transactions with heightened money laundering or counter-terrorist financing risks.

It also requires you to report suspicious transactions.

This chapter highlights a number of warning signs for lawyers and for notaries generally and for those working in specific sectors, to help you decide whether you have reasons for concern or the basis for a disclosable suspicion.

11.2 General warning signs

Because money launderers are always developing new techniques, no list of examples can be fully comprehensive; however, here are some key factors which may heighten a client's risk profile or give you cause for concern.

11.2.1 Secretive clients

While face-to-face contact with clients is not always necessary, an excessively obstructive or secretive client may be a cause for concern.

11.2.2 Unusual instructions

Instructions that are unusual in themselves or that are unusual for your firm or your client may give rise to a cause for concern.

11.2.2.1 Instructions outside your firm's area of expertise.

Taking on work which is outside your firm's normal range of expertise can be risky because money launderers might use such firms to avoid answering too many questions. An inexperienced lawyer or notary might be influenced into taking steps which a more experienced lawyer or notary would not contemplate. Be wary of instructions in niche areas of work in which your firm has no background, but in which the client claims to be an expert.

If your client is based a long way from your offices, consider why you have been instructed. For example, have your services been recommended by another client or is the matter based near your firm? Making these types of enquiries makes good business sense as well as being a sensible anti-money laundering check.

11.2.2.2 Changing instructions

Instructions or cases that change unexpectedly might be suspicious, especially if there seems to be no logical reason for the changes.

The following situations could give rise to a cause for concern.

- a client deposits funds into your client account but then ends the transaction for no apparent reason
- a client tells you that funds are coming from one source and at the last minute the source changes
- a client unexpectedly asks you to send money received into your client account back to its source, to the client or to a third party

11.2.2.3 Unusual retainers

Be wary of:

- disputes which are settled too easily as this may indicate sham litigation
- loss-making transactions where the loss is avoidable
- dealing with money or property where you suspect that either is being transferred to avoid the attention of a trustee in a bankruptcy case, the tax office, or a law enforcement agency
- settlements paid in cash, or paid directly between parties – for example, if cash is passed directly between sellers and buyers without adequate explanation, it is possible that mortgage fraud or tax evasion is taking place
- complex or unusually large transactions
- unusual patterns of transactions which have no apparent economic purpose

11.2.3 Use of client accounts

Only use client accounts to hold client money for legitimate transactions for clients, or for another proper legal purpose. Putting dirty money through a lawyer's or notary's client account can clean it, whether the money is sent back to the client, on to a third party, or invested in some way. Introducing cash into a banking system can become part of the placement stage of money laundering. Therefore, the use of cash may be a warning sign.

Lawyers and notaries should not provide a banking service for their clients. However, it can be difficult to draw a distinction between holding client money for a legitimate transaction and acting more like a bank.

For example, when the proceeds of a sale are left with your firm to make payments, these payments may be to mainstream loan companies, but they may also be to more obscure recipients, including private individuals, whose identity is difficult or impossible to check.

11.2.3.1 Establish a policy on handling cash

Large payments made in actual cash may also be a sign of money laundering. It is good practice to establish a policy of not accepting cash payments above a certain limit either at your office or into your bank account.

Clients may attempt to circumvent such a policy by depositing cash directly into your client account at a bank. You may consider advising clients in such circumstances that they might encounter a delay in completion of the final transaction. Avoid disclosing your client account details as far as possible and make it clear that electronic transfer of funds is expected.

If a cash deposit is received, you will need to consider whether you think there is a risk of money laundering taking place and whether it is a circumstance requiring a disclosure to the GFIU.

11.2.3.2 Source of funds

Accounts staff should monitor whether funds received from clients are from credible sources. For example, it is reasonable for monies to be received from a company if your client is a director of that company and has the authority to use company money for the transaction.

However, if funding is from a source other than your client, you may need to make further enquiries, especially if the client has not told you what they intend to do with the funds before depositing them into your account. If you decide to accept funds from a third party, perhaps because time is short, ask how and why the third party is helping with the funding.

You do not have to make enquiries into every source of funding from other parties. However, you must always be alert to warning signs and in some cases, you will need to get more information.

In some circumstances, cleared funds will be essential for transactions and clients may want to provide cash to meet a completion deadline. Assess the risk in these cases and ask questions if necessary.

11.2.3.3 Disclosing client account details

Think carefully before you disclose your client account details. They allow money to be deposited into your accounts without your knowledge. If you need to provide your account details, ask the client where the funds will be coming from. Will it be an account in their name, from Gibraltar or abroad? Consider whether you are prepared to accept funds from any source that you are concerned about.

Keep the circulation of client account details to a minimum. Discourage clients from passing the details on to third parties and ask them to use the account details only for previously agreed purposes.

11.2.4 Suspect territory

While there are only two countries, namely Iran and North Korea, listed on FATF non cooperative and compliant territories list at the date of issue of these Guidance Notes, this does not mean that all countries that do not appear in that list have anti-money laundering standards equivalent to those in Gibraltar.

Retainers involving countries which do not have comparative money laundering standards may increase the risk profile of the retainer.

Consider whether extra precautions should be taken when dealing with funds or clients from a particular jurisdiction. This is especially important if the client or funds come from a jurisdiction where the production of drugs, drug trafficking, terrorism or corruption is prevalent.

The FATF regularly provides statements on unsatisfactory money laundering controls in overseas jurisdictions.

You should refer to the FATF website and undertake enhanced due diligence and ongoing monitoring with respect to these countries.

The International Bar Association provides a summary of money laundering legislation around the world at: www.anti-moneylaundering.org

Transparency International provides a corruption perception index which may help when you are considering dealing with clients from other countries. It is available at:

http://www.transparency.org/research/cpi/overview

11.3 Private client work

11.3.1 Administration of estates

The administration of estates will be a regulated activity under the Legal Services Act. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for laundering their funds; however, there is still a low risk of money laundering for those working in this area.

11.3.1.1 Source of funds

When you are acting either as an executor, or for executors, there is no blanket requirement that you should be satisfied about the history of all of the funds which make up the estate under administration; however, you should be aware of the factors which can increase money laundering risks.

Consider the following when administering an estate:

- where estate assets have been earned in a foreign jurisdiction, be aware of the wide definition of criminal conduct in POCA and the provisions relating to overseas criminal conduct
- where estate assets have been earned or are located in a suspect territory, you may need to make further checks about the source of those funds

The wide nature of the offences of 'acquisition, use and possession' in section 3 POCA may lead to a money laundering offence being committed at an early point in the administration. The section 2(1) POCA offence may also be relevant.

Be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed and problems of delayed consent are avoided. A key benefit of the judgment in *Bowman v Fels* (cited above) is that a lawyer who makes a disclosure is now able to continue work on the matter, so long as they do not transfer funds or take any other irrevocable step.

11.3.1.2 How the estate may include criminal property

An extreme example would be where you know or suspect that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

If you know or suspect that the deceased person improperly claimed welfare benefits or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a money laundering disclosure may be required. When working with UK clients for example information on the financial thresholds for benefits can be obtained from www.dwp.gov.uk or www.hmrc.gov.uk. For Gibraltar residents, information is available from the Government website at https://www.gibraltar.gov.gi.

While administering an estate, you may discover or suspect that beneficiaries are not intending to pay the correct amount of tax or are avoiding some other financial charge (for example, avoiding Gibraltar tax due by failing to disclose gifts received from the deceased less than seven years before death). Although these matters may not actually constitute money laundering (because no criminal conduct has yet occurred so there is no 'criminal property'), you should carefully consider their position in conduct terms with respect to the Applicable Codes.

11.3.1.3 Grant of probate

A Gibraltar grant of probate may be required before Gibraltar assets can be released, while for overseas assets the relevant local laws will apply. Remain alert to warning signs, for example if the deceased or their business interests are based in a suspect territory.

If the deceased person is from another jurisdiction and a lawyer is dealing with the matter in the home country, it may be helpful to ask that person for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

11.3.2 Trusts

Trust work is a regulated activity.

Trusts can be used as a money laundering vehicle. The key risk period for trusts is when the trust is set up, as if the funds going into the trust are clean, it is only by the trustees using them for criminal purposes that they may form the proceeds of crime.

When setting up a trust, be aware of general money laundering warning signs and consider whether the purpose of the trust could be to launder criminal property. Information about the purpose of the trust, including why any unusual structure or jurisdiction has been used, can help allay concerns. Similarly, information about the provider of the funds and those who have control of the funds, as required by the POCA, will assist.

Whether you act as a trustee yourself, or for trustees, the nature of the work may already require information which will help in assessing money laundering risks, such as the location of assets and the identity of trustees. Again, any involvement of a suspect jurisdiction, especially those with strict bank secrecy and confidentiality rules, or without similar money laundering procedures, may increase the risk profile of the retainer.

If you think a money laundering offence has, or may have, been committed that relates to money or property which already forms part of the trust property, or is intended to do so, consider whether your instructions involve you in a section 2(1) POCA arrangement offence. If they do, consider the options for making a disclosure.

11.3.3 Charities

In common with trusts, while the majority of charities are used for legitimate reasons, they can be used as money laundering/terrorist financing vehicles.

If you are acting for a charity, consider its purpose and the organisations it is aligned with. If you are receiving money on the charity's behalf from an individual or a company donor, or a bequest from an estate, be alert to unusual circumstances including large sums of money.

11.3.4 Powers of attorney/deputyship

Whether acting as, or on behalf of, an attorney or deputy, you should remain alert to money laundering risks.

If you are acting as an attorney you may learn financial information about the donor relating, for example, to non-payment of tax or wrongful receipt of benefits. You will need to consider whether to make a disclosure to the GFIU.

Where the public guardian has an interest - because of a deputyship or registered enduring power of attorney - consider whether the Registrar of the Court of Protection needs to be informed. Informing the Registrar of the Court of Protection is unlikely to be tipping-off because it is unlikely to prejudice an investigation.

If you discover or suspect that a donee has already completed an improper financial transaction that may amount to a money laundering suspicion, a disclosure to the GFIU may be required (depending on whether legal professional privilege applies). However, it may be difficult to decide whether you have a suspicion if the background to the information is a family dispute.

11.4 Property work

11.4.1 Ownership issues

Properties owned by nominee companies or multiple owners may be used as money laundering vehicles to disguise the true owner and/or confuse the audit trail.

Be alert to sudden or unexplained changes in ownership. One form of laundering, known as flipping, involves a property purchase, often using someone else's identity. The property is then quickly sold for a much higher price to the same buyer using another identity. The proceeds of crime are mixed with mortgage funds for the purchase. This process may be repeated several times.

Another potential cause for concern is where a third party is providing the funding for a purchase, but the property is being registered in someone else's name. There may be legitimate reasons for this, such as a family arrangement, but you should be alert to the possibility of being misled about the true ownership of the property. You may wish to undertake further CDD measures on the person providing the funding.

11.4.2 Methods of funding

Many properties are bought with a combination of deposit, mortgage and/or equity from a current property. Usually, as a lawyer, you will have information about how your client intends to fund the transaction, and will expect to be updated if those details change, for example if a mortgage falls through and new funding is obtained.

This is a sensible risk assessment measure which should help you decide whether you need to know more about the transaction.

11.4.2.1 Private funding

Usually purchase funds comprise some private funding, with the majority of the purchase price being provided via a mortgage. Transactions that do not involve a mortgage have a higher risk of being fraudulent.

Look out for:

- large payments from private funds, especially if your client has a low income
- payments from a number of individuals or sources If you are concerned:
- ask your client to explain the source of the funds. Assess whether you think their explanation is valid - for example, the money may have been received from an inheritance or from the sale of another property
- consider whether the beneficial owners were involved in the transaction

Remember that payments made through the mainstream banking system are not guaranteed to be clean.

11.4.2.2 Funds from a third party

Third parties often assist with purchases, for example relatives often assist first time home buyers. You may be asked to receive funds directly from those third parties. You will need to decide whether, and to what extent, you need to undertake any CDD measures in relation to the third parties.

- Consider whether there are any obvious warning signs and what you know about:
- your client
- the third party
- their relationship
- the proportion of the funding being provided by the third party

Consider your obligations to the lender in these circumstances – you are normally required to advise lenders if the buyers are not funding the balance of the price from their own resources.

11.4.2.3 Direct payments between buyers and sellers

You may discover or suspect that cash has changed hands directly, between a seller and a buyer, for example at a rural auction.

If you are asked to bank the cash in your client account, this presents a problem because the source of the cash is not your client and so checks on the source of the funding can be more difficult. The auction house may be able to assist because of checks they must make under applicable legislation. However, you may decide to decline the request.

If you suspect that there has been a direct payment between a seller and a buyer, consider whether there are any reasons for concern (for example, an attempt to involve you in tax evasion) or whether the documentation will include the true purchase price.

A client may tell you that money is changing hands directly when this is not the case. This could be to encourage a mortgage lender to lend more than they would otherwise, because they believe that private funds will contribute to the purchase. In this situation, consider your duties to the lender.

11.4.3 Valuing

An unusual sale price can be an indicator of money laundering. While you are not required to get independent valuations, if you become aware of a significant discrepancy between the sale price and what you would reasonably expect such a property to sell for, consider asking more questions.

Properties may also be sold below the market value to an associate, with a view to obscuring the title to the property while the original owner still maintains beneficial ownership.

11.4.4 Lender issues

You may discover or suspect that a client is attempting to mislead a lender client to improperly inflate a mortgage advance - for example, by misrepresenting the borrower's income or because the seller and buyer are conspiring to overstate the sale price. Transactions which are not at arm’s length may warrant particularly close consideration.

However, until the improperly obtained mortgage advance is received there is not any criminal property for the purposes of disclosure obligations under POCA.

If you suspect that your client is making a misrepresentation to a mortgagee you must either dissuade them from doing so or consider the ethical implications of continuing with the retainer (see in particular your obligations under the Applicable Codes). Even if you no longer act for the client you may still be under a duty to advise the mortgage company.

If you discover or suspect that a mortgage advance has already been improperly obtained, consider advising the mortgage lender.

If you are acting in a re-mortgage and discover or suspect that a previous mortgage has been improperly obtained, you may need to advise the lender, especially if the re-mortgage is with the same lender. You may also need to consider making a disclosure to the GFIU as there is criminal property (the improperly obtained mortgage advance).

11.4.4.1 Legal professional privilege

If your client has made a deliberate misrepresentation on their mortgage application you should consider whether the crime/fraud exemption to legal professional privilege will apply, so that no waiver to confidentiality will be needed before a disclosure is made.

However, you will need to consider matters on a case-by-case basis and if necessary, seek legal advice.

11.4.4.2 Tipping-off offences

You may be concerned that speaking to the lender client conflicts with tipping-off offences.

A key element of these offences is the likelihood of prejudicing an investigation. The risk of this is small when disclosing to a reputable lender or your insurer. The financial services sector is also regulated for the purposes of anti-money laundering and subject to the same obligations. There is also a specific defence of making a disclosure for the purposes of preventing a money laundering offence.

In relation to asking further questions of your client and discussing the implications of POCA, there is a specific defence for tipping-off for legal advisers who are seeking to dissuade their client from engaging in a money laundering offence.

For further advice on tipping-off, see chapter 5.7 of these Guidance Notes.

For further information about avoiding tipping-off in a particular case, contact the GFIU on +350 200 70211.

11.4.5 Tax issues

Tax evasion of any type, whether committed by your client or the other party to a transaction, can result in you committing a section 2(1) POCA arrangements offence.

Abuse of the Stamp Duties Act 2005 procedure may also have money laundering implications, for example if the purchase price is recorded incorrectly.

If a client gives you instructions which offend the Stamp Duties Act 2005 procedure, you must consider your position under the Applicable Codes. If you discover the evasion after it has occurred, you are obliged to make a disclosure, subject to any legal professional privilege.

11.5 Company and commercial work

The nature of company structures can make them attractive to money launderers because it is possible to obscure true ownership and protect assets for relatively little expense. For this reason, lawyers and notaries working with companies and in commercial transactions should remain alert throughout their retainers, with existing as well as new clients.

11.5.1 Forming a new company

If you work on the formation of a new company, be alert to any signs that it might be misused for money laundering or terrorist financing.

If the company is being formed in a foreign jurisdiction, it may be helpful to clarify why this is the case. In countries where there are few anti-money laundering requirements, you should make particularly careful checks.

If you are in doubt, it may be better to refuse the retainer.

11.5.2 Holding of funds

If you wish to hold funds as stakeholder or escrow agent in commercial transactions, consider the checks you wish to make about the funds you intend to hold, before the funds are received and whether it would be appropriate to conduct CDD measures on all those on whose behalf you are holding funds.

Consider any proposal that you collect funds from a number of individuals, whether for investment purposes or otherwise. This could lead to wide circulation of your client account details and payments being received from unknown sources.

11.5.3 Private equity

Law firms could be involved in any of the following circumstances:

- the start-up phase of a private equity business where individuals or companies seek to establish a private equity firm (and in certain cases, become authorised to conduct investment business)
- the formation of a private equity fund
- ongoing legal issues relating to a private equity fund
- execution of transactions on behalf of a member of a private equity firm's group of companies, (a private equity sponsor), that will normally involve a vehicle company acting on its behalf, ("Newco")

11.5.3.1 Who is the client?

Start-up phase

In this phase, as you will be approached by individuals or a company seeking to become established (and in certain cases authorised) your client would be the individuals or company and you would therefore conduct CDD accordingly.

Formation of private equity funds

Your client is likely to be the private equity sponsor or it may be an independent sponsor.

You will rarely, if ever, be advising the fund itself and, unless you are instructed directly by an investor, you will not be considered to be advising the investors in the fund.

You should therefore identify who your client is and apply the CDD measures according to their client type as set out in chapter 4.6 of these Guidance Notes.

Where the client is a Newco, you will need to obtain documentation evidencing the establishment of the Newco and consider the issue of beneficial ownership.

Generally private equity work will be considered at low risk of money laundering or terrorist financing for the following reasons:

- private equity firms in Gibraltar may also covered by POCA as a relevant financial business and would be regulated by the GFSC
- investors in private equity funds are generally large institutions, some of which will also be regulated for money laundering purposes. They will have long established relationships with the private equity firm, usually resulting in a well-known investor base
- where the private equity sponsor or fund manager is regulated in Gibraltar, EEA or comparable jurisdictions, it is likely to have followed CDD processes prior to investors being accepted
- the investment is generally illiquid and the return of capital is unpredictable
- the terms of the fund documentation generally strictly control the transfer of interests and the return of funds to investors

Factors which may alter this risk assessment include:

- where the private equity sponsor or an investor is located in a jurisdiction which is not regulated for money laundering to a standard which is equivalent to the 4MLD
- where the investor is either an individual or an investment vehicle itself (a private equity fund of funds)
- where the private equity sponsor is seeking to raise funds for the first time

JMLSG has prepared detailed advice on CDD measures for private equity businesses in Part II of its guidance, which you may wish to consider. See chapter 4.3.4 of these Guidance Notes.

The following points should be considered when undertaking CDD measures in relation to private equity work:

- where your client qualifies for simplified due diligence you do not have to identify beneficial owners unless there is a suspicion of money laundering
- where simplified due diligence does not apply you need to consider the business structure of the client and conduct CDD on the client in accordance with that structure
- where there is an appropriately regulated professional closely involved with the client who has detailed knowledge of the beneficial owners of the client, you may consider relying on them in accordance with Chapter II, Article 25 of the 4MLD
- whether an unregulated private entity firm, fund manager or other person involved with the transaction is an appropriate source of information regarding beneficial ownership of the client should be determined on a risk-sensitive basis, issues to consider include:
    - the profile of the private equity sponsor, fund manager, (if different), or such other person
    - their track record within the private equity sector
- their willingness to explain identification procedures and provide confirmation that all beneficial owners have been identified
- where you are using another person as an information source for beneficial owners, where there are no beneficial owners within the meaning of Article 3(6) of 4MLD, the source may simply confirm their actual knowledge of this, or if beneficial owners do exist, the source should provide you with the identifying details of the beneficial owner or an assurance that the beneficial owners have been identified and that the details will be provided on request.
- where there is a tiered structure, such as a feeder fund or fund of funds structure, you must identify the beneficial owner but you may decide having made enquiries that no such beneficial owners exist even though you have got to the top of the structure.
- where it is envisaged that you will be acting for a Newco which is to be utilised at a future point in a flotation or acquisition, it is only once they are established and signed up as a party to the transaction that you need to commence CDD measures on the Newco. However, once you start acting for a Newco, you will need to consider identification for it, and its beneficial owner. You may therefore wish to commence the process of identifying any beneficial owner in advance.

11.5.4 Collective investment schemes

Undertaking work in relation to retainers involving collective investment schemes may pose similar problems when undertaking CDD as for private equity work.

The risk factors with respect to a collective investment scheme will be decreased where:

- the scheme is only open to tax exempt institutional investors
- the scheme is only open to institutional investors
- investment managers are regulated individuals or entities
- a prospectus is issued to invite investment

Factors which will increase the risks include where:

- the scheme is open to non-institutional investors

- the scheme or its investors are located in a jurisdiction which is not regulated for money laundering to a standard which is equivalent to the 4MLD
- neither the scheme nor the investment managers are regulated and do not conduct CDD on the investors

JMLSG have also issued guidance which touches on the area of collective investment schemes, which you may wish to have regard to. See chapter 4.3.4 of these Guidance Notes.

In addition to the points to consider outlined for private equity work, where a collective investment scheme has issued a prospectus it is advisable to review a copy of the prospectus to understand the intended structure of the investment scheme.

Chapter 12 Offences & Reporting Practical Examples

12.1 General Comments

Chapters 5 and 6 of these Guidance Notes worked through the theory of the law relating to when a money laundering offence has occurred, the requirements for making a disclosure and when you are unable to make a disclosure because of LPP.

This chapter contains examples to help put the theory into context

This chapter does not replace application of the legislation to your situation; nor should it be viewed without reference to the detailed discussion of the law in the rest of the practice note.

Further examples may be added to future editions of these Guidance Notes.

12.2 Principal offences

If you suspect that property involved in a retainer is criminal property, offences under section 4 and section 3 of POCA are relatively straightforward to assess. However, an arrangement offence under section 2(1) POCA may be more complicated, particularly with transactional matters.

12.2.1 Do I have an arrangement?

Under section 2(1) POCA, an arrangement must be created at a particular point in time. If you have formed a suspicion, first consider whether an arrangement already exists. For example, a client may instruct you to act for them in the purchase of a property, including the drafting of the contract and transfer documents. When you are instructed there will already an arrangement between the vendor and the purchaser, but not yet an arrangement for the purposes of section 2(1) POCA.

If an arrangement within section 2(1) POCA already exists, any steps you take to further that arrangement will probably mean you are concerned in it. In this case, you would immediately need to consider making a disclosure.

12.2.2 No pre-existing arrangement

If there is no pre-existing arrangement, the transactional work you carry out may bring an arrangement under section 2(1) POCA into existence. You may become concerned in the arrangement by, for example, executing or implementing it, which may lead you to commit an offence under section 2(1) POCA, and possibly under section 4 or 3 of POCA.

Consider whether you need to make an authorised disclosure to:

- obtain consent to proceed with the transaction
- provide yourself with a defence to the principal money laundering offences

If you are acting within a relevant financial business, consider whether you risk committing a failure to disclose offence, if you do not make a disclosure to the GFIU.

The following two flowcharts show the issues to consider when deciding whether to make a disclosure to the GFIU.

12.3 Should I make a disclosure?

12.3.1 Property transactions

Considering further the earlier example of a suspect contract for the purchase of a property, the following issues will be relevant when considering the disclosure requirements under POCA.

- If the information on which your suspicion is based is covered by LPP and the crime/fraud exception does not apply, you cannot make a disclosure under POCA.
- If neither of these situations applies, the communication will still be confidential. However, the material is disclosable under POCA and an authorised disclosure should be made

You have the option of withdrawing from the transaction rather than making an authorised disclosure, but you may still need to make a disclosure to avoid committing a failure to disclose offence.

What if I cannot disclose?

If you decide that either you cannot make a disclosure due to LPP, you have two options:

- you can approach the client for a waiver of privilege to make a disclosure and obtain consent to carry out the prohibited act, or
- you should consider your ethical obligations and whether you need to withdraw from the transaction (refer to the Applicable Codes).

Waiver of privilege

When approaching your client for a waiver of privilege, you may feel less concerned about tipping-off issues if your client is not the suspect party but is engaged in a transaction which involves criminal property. However, if you suspect that your client is implicated in the underlying criminal conduct, consider the tipping-off offence and whether it is appropriate to discuss these matters openly with your client.

If you raise the matter with your client and they agree to waive privilege, you can make a disclosure to the GFIU on your own or jointly with your client and seek consent if required.

If you are acting for more than one client on a matter, all clients must agree to waive privilege before you can make a disclosure to the GFIU.

Refusal to waive privilege

Your client, whether sole or one of a number for whom you act, may refuse to waive privilege, either because he does not agree with your suspicions or because he does not wish a disclosure to be made. Unless your client provides further information which removes your suspicions, you must decide whether you are being used in a criminal offence, in which case LPP does not apply.

If your client refuses to waive privilege but accepts that in proceeding with the transaction he may be committing an offence, you might conclude that you are being used in a criminal offence in which case neither exemption applies. In such circumstances it is not appropriate to tell the client that you are making the disclosure, as the risks of tipping-off are increased.

If you are unable to make a disclosure, consider the ethical and civil risks of continuing in the retainer and consider withdrawing.

Consent and progressing the retainer

If you make a disclosure and consent is needed, consider whether you can continue working on the retainer before you receive that consent.

This will depend on whether an arrangement already exists or whether the further work will bring the arrangement into existence. Provided there is no pre-existing arrangement you should be free to continue your preparatory activities. However, the arrangement/prohibited act should not be finalised without appropriate consent.

12.3.2 Company transactions

Criminal property in a company

The extent of the regulatory and legal obligations affecting companies and businesses means that there is an increased possibility that breaches will have been committed by your client that constitute criminal conduct and give rise to criminal property under POCA.

For example, the Companies Act 2014 contains certain offences which will give rise to criminal property as defined by POCA. There does not need to be a criminal conviction, nor even a prosecution underway. If criminal conduct has, (or is suspected to have) taken place, and a benefit has been achieved, the result is actual or notional criminal property.

For a number of offences, the only benefit to your client (for the purposes of POCA) is saved costs. For example, it is criminal conduct to fail to notify the Data Protection Commissioner that a company will be processing 'personal data'. The saved notification fee should be treated as criminal property for the purposes of POCA.

It may be difficult to establish whether property or funds which are the subject of the transactions are the 'saved costs' in whole or in part and are therefore tainted. If you are dealing with the whole of a company's business or assets, no distinction is necessary. In other cases, it would be wrong to assume that because some assets are tainted, they all are, or that you are dealing with the tainted ones.

In most cases, unless there is some basis for suspecting that the assets in question result from saved costs, no disclosure/consent may be required in respect of the principal offence. However, a disclosure may still be required in respect of the failure to disclose offences

Mergers and acquisitions

In typical corporate merger/acquisition/sale/take-over transactions, there are a number of issues to consider.

Lawyers and notaries acting in company transactions will be acting in a relevant financial business and so will have dual disclosure obligations, under the failure to disclose offence and in respect of the principal offences.

Different tests have to be applied to determine whether a disclosure can be made. When you are considering whether you are obliged to make a disclosure to avoid committing a failure to disclose offence, either LPP or privileged circumstances may apply.

When you are considering whether you must make a disclosure as a defence to the principal offences, only LPP is relevant.

For example, when you are acting for a vendor, you may receive information from the client about the target company which is protected under LPP and exempt from disclosure due to privileged circumstances. However, you may receive information from other representatives of the client (such as other professional advisers) which may only be exempt due to privileged circumstances. If information received is initially privileged, you need to consider whether the privilege is lost in the course of the transaction.

The information may be put into a data room and the purchaser, as part of the due diligence inquiries, may raise questions of the vendor's lawyers which, in effect, result in the information being received again by the vendor's lawyer.

That second receipt from the purchaser, or their lawyer, would not be protected by privileged circumstances. It will lose its exemption from disclosure unless the information was also subject to LPP which had not been waived when it was placed in the data room (e.g. a letter of advice from a lawyer to the vendor).

Consider whether privilege is removed by the crime/fraud exception. You may suspect, or have reasonable grounds to suspect someone of money laundering (which may simply mean they possess the benefits of a criminal offence contrary to section 3 of POCA). Where the information on which the suspicion is based could be protected by LPP or exempted due to privileged circumstances, consider whether the crime/fraud exception applies. This may depend on:

- the nature of the transaction
- the amount of the criminal property
- the strength of the evidence

These factors are considered in more detail below with respect to specific types of company sales.

Asset sales

In the case of an asset sale, all or some of the assets of the business may be transferred. If any asset transferred to a new owner is criminal property, a money laundering offence may be committed:

- The vendor may commit a section 4 POCA offence by transferring the criminal property.
- Both the vendor and purchaser may be entering into an arrangement contrary to section 2(1) POCA.
- The purchaser may be committing a section 3 POCA offence by possessing the criminal property

Adequate consideration defence

When looking at the purchaser's position, you will need to consider whether there would be an adequate consideration defence to a section 3 POCA possession offence. This is where the purchase price is reasonable and constitutes adequate consideration for any criminal property obtained. In such a case, should the purchaser effectively be deprived of the benefit of that defence by section 2(1) POCA?

It is a question of interpretation whether sections 2(1) and 3 of POCA should be read together such that, if the defence under section 3 POCA applies, an offence will also not be committed by the vendor under section 2(1) POCA. You should consider this point and take legal advice as appropriate.

Disclosure obligations after completion

As well as making disclosures relating to the transaction, vendors and purchasers will need to consider disclosure obligations in respect of the position after completion.

The purchaser will, after the transaction, have possession of the assets and may be at risk of committing a section 3 POCA offence (subject to the adequate consideration defence outlined above).

The vendor will have the sale consideration in their possession. If the amount of the criminal property is material, the sale consideration may indirectly represent the underlying criminal property and the vendor may commit an offence under section 3 POCA.

Whether the criminal property is material or not will depend on its impact on the sale price. For example, the sale price of a group of assets may be £20m. If the tainted assets represent 10 per cent of the total, and the price for the clean assets alone would be £18m, it is clear that the price being paid is affected by, and represents in part, the criminal property.

If a client commits one of the principal money laundering offences, whether you are acting for the vendor or purchaser, you will be involved in a prohibited act. You will need to make a disclosure along with your clients and obtain appropriate consent.

When considering whether to advise your client about their disclosure obligations, remember the tipping-off offences.

Am I prevented from reporting due to LPP?

Where you are acting for either the purchaser or vendor and conclude that you may have to make a disclosure and seek consent, first consider whether LPP applies. As explained above, this depends on how you received the information on which your suspicion is based.

Generally, when acting for the purchaser, if the information comes from the data room, LPP will not apply. When acting for the vendor, LPP may apply if the information has come from the client for the purpose of obtaining legal advice.

The crime/fraud exception

Where LPP applies, you will also need to consider whether the crime/fraud exception applies. The test is whether there is prima facie evidence that you are being used for criminal purposes.

Whether the crime/fraud exception applies will also depend on the purpose of the transaction and the amount of criminal property involved. For example, if a company wished to sell assets worth £100m, which included £25 of criminal assets, it would be deemed that the intention was not to use lawyers for criminal purposes but to undertake a legitimate transaction. However, if the amount of criminal property was £75m, the prima facie evidence would be that the company did intend to sell criminal property and the exception would apply to override LPP.

Real cases will not all be so clear-cut. Consider the parties' intentions. If you advise your client of money laundering risks in proceeding with a transaction and the client decides, despite the risks, to continue without making a disclosure, you may have grounds to conclude that there was prima facie evidence of an intention to use your services for criminal purposes and therefore that privilege may be overridden.

Remember that for the purposes of the crime/fraud exception, it is not just the client's intention that is relevant.

Where LPP applies and is not overridden by the crime/fraud exception, it is nonetheless possible for your client to waive the privilege in order for a disclosure to be made.

Share sales

A sale of a company by way of shares gives rise to different considerations to asset sales. Unless shares have been bought using the proceeds of crime, they are unlikely to represent criminal property, so their transfer will not usually constitute a section 4 POCA offence, (for the vendor), or a section 3 POCA offence, (for the purchaser).

However, the sale of shares could constitute a section 2(1) POCA offence, depending on the circumstances, particularly if the criminal property represents a large percentage of the value of the target company. Consent may be needed if:

- the benefit to the target company from the criminal conduct is such that its share price has increased

- as part of the transaction directors will be appointed to the board of the target company and they will use or possess criminal property
- the purpose of the transaction is to launder criminal property. That is, it is not a genuine commercial transaction.

Is the share value affected by criminal property?

If a company has been used to commit criminal offences, some or all of its assets may represent criminal property. The value of the shares may have increased as a result of that criminal activity. When the shares are then sold, by converting a paper profit into cash, the vendor and the purchaser have both been involved in a prohibited arrangement

For example, if 10 per cent of the profits of a company are earned from criminal activity, it is likely that the share price would be lower if only the legitimate profits were taken into account.

However, if the value of the criminal property is not sufficient to affect the purchase/sale price, the transaction is unlikely to be considered a prohibited arrangement since the vendor does not benefit from the company's criminal conduct. For example, a company is being purchased for £100m and within it is £25 of saved costs. If the costs had been paid by the company, it is unlikely that the price would be £99,999,975. The business is still likely to be valued at £100m.

Where criminal property is immaterial

Even if the value of criminal property is very small and immaterial to the purchase price, purchasers still need to consider their position after the acquisition. While shareholders do not possess a company's assets, the target company and directors may subsequently transfer, use or possess the assets for the purposes of the principal money laundering offences in sections 3 and 4 of POCA.

If as part of the transaction, the purchaser proposes appointing new directors to the board of the target company, those directors may need to make a disclosure and seek consent so that they may transfer use or possess and use the criminal property.

In this case, you, and the vendors and the existing and new directors, may still need to make a disclosure, (subject to LPP issues), and seek consent, because they will be involved in an arrangement which involves the acquisition, use or control of criminal property by the new directors contrary to section 2(1) POCA.

In summary, the position may be as follows where the amount of the criminal property is immaterial:

- The target company will possess the proceeds of criminal conduct and may need to make a disclosure. If you discover this in privileged circumstances or it is protected by LPP, you cannot make a disclosure unless the fraud/crime exception applies.
- Those individuals or entities which, as a result of the transaction, will be in a position after completion to possess and use criminal property will need to make a disclosure and seek consent before completion.
- The lawyers acting on the transaction and the vendor may also need to make a disclosure if they are involved in an arrangement which facilitates the acquisition or use of criminal property.
- Whenever a disclosure must be made, you must first consider whether privilege applies and, if applicable, whether the fraud/crime exception applies

Shareholders

Generally, in a purchase or sale transaction, you will act for the company, not for its shareholders. However, it is possible for shareholders to become involved in an arrangement prohibited by section 2(1) POCA.

Firstly, consider whether the shareholders are, or may become, aware – perhaps through the risk warnings in the circular – of the risk of criminal conduct. Unless they are so aware, they are unlikely to have the necessary suspicion to be at risk of committing a money laundering offence.

Secondly, where shareholders are aware of the criminal conduct, consider whether the amount of criminal property is material to the transaction. That is, it would have an impact on the price or terms. If it is material, by voting in favour of it the shareholders will become concerned in a prohibited arrangement and will be required to make a disclosure and seek consent.

Also consider, in the context of an initial public offering, what risk warnings to include in any prospectus. You may need to give shareholders notice of their disclosure obligations via such a risk warning.

It is good practice to discuss the issue with the GFIU to ensure that there are no tipping-off concerns if details of the risks are set out in the public circular.

When each shareholder requires consent from the GFIU, their express authority to make the disclosure will be required. It may be simplest to ask the shareholders to authorise the board of the vendor to make a disclosure and seek consent on their behalf at the same time as asking them to give conditional approval for the transaction.

Overseas conduct

Where your suspicion of criminal conduct relates in whole or in part to overseas conduct, be aware of the wide definition of criminal conduct.

For example, you might discover or suspect that a company or its foreign subsidiary has improperly manipulated its accounting procedures so that tax is paid in a country with lower tax limits. Or you might form a concern about corrupt payments to overseas commercial agents which might be illegal in Gibraltar.

Even where the conduct is lawful overseas, in serious cases it will still be disclosable if the money laundering is taking place in Gibraltar and the underlying conduct would be criminal if it had occurred in Gibraltar.

In some cases, the only money laundering activity in Gibraltar may be your involvement in the transaction as a Gibraltar lawyer or Gibraltar notary.

Published by:

The Registrar of the Supreme Court
Supreme Court
277 Main Street
Gibraltar

Tel: (+350) 200 75608 (Registry)
(+350) 200 78808 (Registrar)
Fax: (+350) 200 77118

1st November 2017