4MLD AND AMENDMENTS TO POCA

August 2017

This newsletter covers amendments made to the Proceeds of Crime Act 2015 (POCA) as well the introduction and amendments to secondary legislation made since late 2016, in particular;

LN		Name
256	2016	Proceeds of Crime Act 2015 (Amendment) Regulations 2016
115	2017	Supervisory Bodies (Powers, etc) Regulations 2017
119	2017	Proceeds of Crime Act 2015 (Amendment) Regulations 2017
120	2017	National Coordinator for Anti-Money Laundering and Combatting the Financing of Terrorism (Amendment) Regulations 2017
Act		Name
7	2017	Proceeds of Crime (Amendment) Act 2017

A TIME FOR CHANGE

The transposition of 4MLD has required substantial amendments to the Proceeds of Crime Act 2015. This newsletter highlights the main changes that regulated entities should take into consideration when reviewing and implementing systems of control to meet these new requirements. HMGoG has also taken this opportunity to review exisiting provisions and make some additional, non 4MLD specific updates to the legislation so that Gibraltar's AML/CFT legislation remains current with international standards.

This newsletter is neither an exhaustive nor authoritative commentary on all the amendments.

This newsletter is not, however, a substitute for seeking professional advice and has no legal standing.

THE REVISED MONEY LAUNDERING OFFENCES

The Mental Elements

The mental elements which are relevant to the ML offences under POCA are:

- knowledge
- suspicion
- reasonable grounds for suspicion

These are the three mental elements in the offences, although the third one only applies to offences relating to the regulated sector. 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. This defence is not available in criminal proceedings,

The principal money laundering offences, ie Sections 2, 3 and 4, each require proof that the conduct concerned "criminal property". In order to prove that the property is "criminal property" it has to be shown that the alleged offender knows or suspects that the property constitutes the benefit from criminal conduct. For an offence under Section 2 to be proved the alleged offender must additionally know or suspect that his actions will facilitate any arrangements in respect of criminal property.

For an offence to be proved under section 6B, failing to disclose money laundering within the relevant financial business sector, it has to be proved that the alleged offender knows, suspects or has reasonable grounds to suspect that another person is engaged in or attempting to

launder money. 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.

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

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 [2006] 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.

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.

Reasonable grounds to suspect
The issues here for the relevant financial business 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?

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.

Section 4 - Concealing
A person commits an offence if he conceals, disguises, converts, or transfers criminal property, or removes 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.

Section 3 – Acquisition, possession or use
A person commits an offence if he acquires criminal property, uses criminal property or has possession of criminal property.

Section 2 - Arrangements
A person commits an offence if he enters into, or becomes concerned in an arrangement which he knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.

This is the offence which will often be apt for the prosecution of those who launder on behalf of others.

It will catch persons who work in financial or credit institutions, accountants etc, who in the course of their work facilitate money laundering by or on behalf of other persons.

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.

An agreement to make an arrangement will not always be an arrangement but this may be a consipiracy. 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.

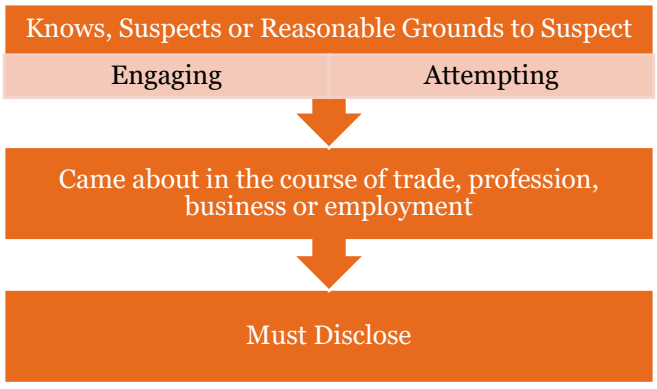
Entering into or becoming concerned in an arrangement
To enter into an arrangement is to become a party to it.

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.

Section 5 – Tipping Off
There have been no amendments to this offence.

Section 6B – Failure to disclose: Relevant financial businesses
This is not a new offence as it existed in POCA prior to the amendments coming into force. It was felt, however, that it made more sense to have it as a separate offence.



It places a duty on employees in a relevant financial business to make reports where they "know or suspect" that another person is engaged in money laundering and where (even if they do not know or suspect) they "have reasonable grounds for knowing or suspecting" that a person is engaged in money laundering.

The "reasonable grounds for knowing or suspecting" standard (i.e. a "should have known" or negligence test) is very important. The rationale for this is that a higher standard of diligence is expected in anti-money laundering prevention in the regulated sector, where comprehensive preventive systems (in line with international standards), are required to be in place.

Defences to the principal money laundering offences

You will have a defence to a principal money laundering offence if:

- you make an authorised disclosure prior to the offence being committed and you gain appropriate consent (the consent defence)
- you intended to make an authorised disclosure but had a reasonable excuse for not doing so (the reasonable excuse defence)

Authorised Disclosures
Section 4G authorises you to make a disclosure regarding suspicion of money laundering as a defence to the principal money laundering offences.

It specifically provides that you can make a disclosure either

- before money laundering has occurred
- while it is occurring but as soon as you suspect
- after it has occurred, if you had good reason for not disclosing earlier and make the disclosure as soon as practicable

If a disclosure is authorised, it does not breach any requirement which would otherwise restrict it.

Where your firm has appointed an “appropriate person” (MLRO), you should make your disclosure to the MLRO. The nominated officer will consider your disclosure and decide whether to make an external disclosure to the GFIU. If your firm does not have a MLRO, you should make your disclosure directly to the GFIU.

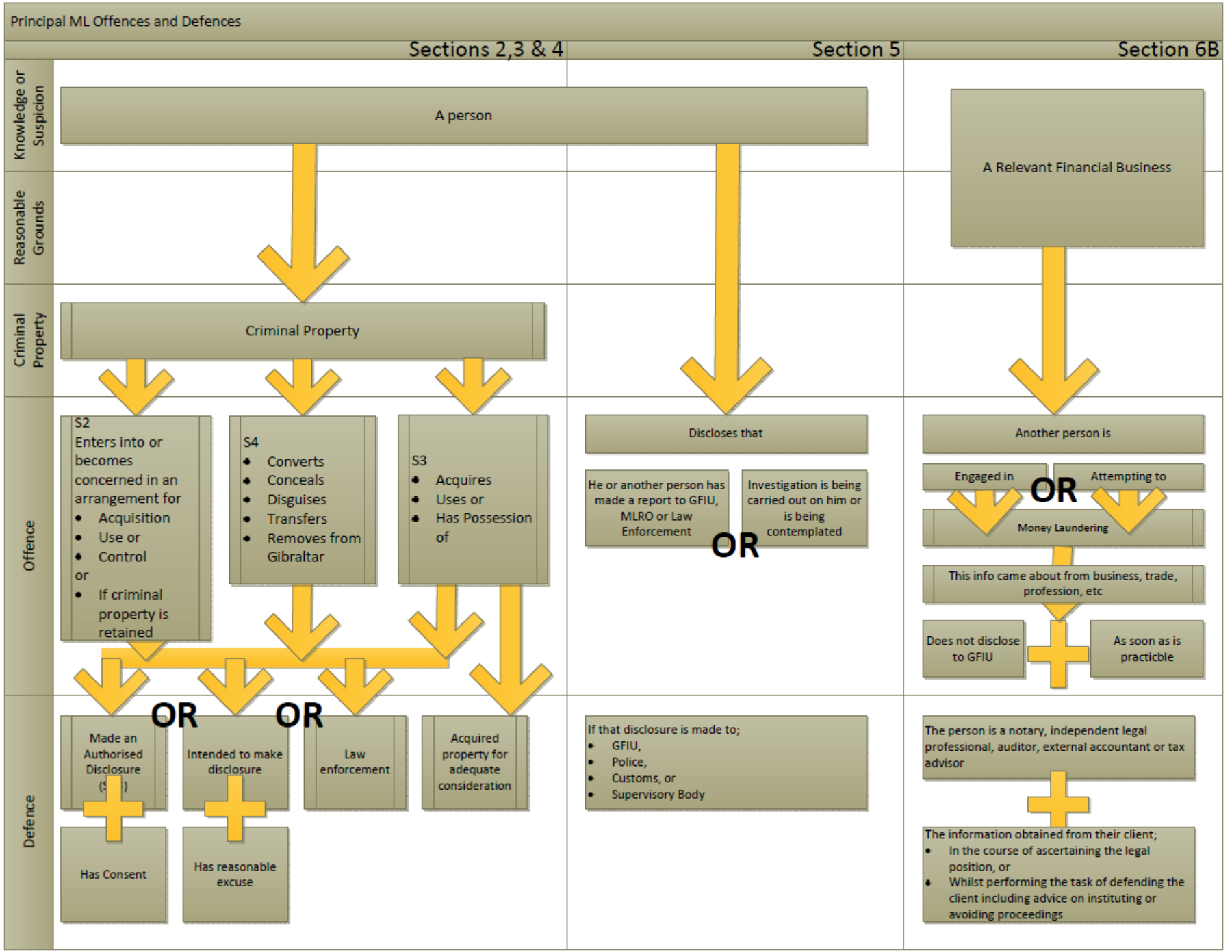
Section 4G(5) gives those making such a disclosure protection from any professional or statutory duty that would otherwise prevent them from making such a disclosure whilst S4G(6) protects the person making the disclosure from civil liability so long as the disclosure is made in good faith.

Reasonable excuse defence
This defence applies where a person intended to make a disclosure before doing a prohibited act, but had a reasonable excuse for not disclosing.

You will have a defence against a principal money laundering offence if you make a disclosure.

Adequate consideration defence
This defence applies in S3(2)(c) 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.

Inadequate consideration is explained in S3(5) and essentially is that a person acquires, uses or has possession of property in exchange for inadequate consideration which is significantly less than the value of the property or the value of the use of the property.


Principal ML Offences and Defences
Sections 2,3 & 4
Section 5
Section 6B
Knowledge or Suspicion
Reasonable Grounds
Criminal Property
Offence
Defence
A person
A Relevant Financial Business
Criminal Property
S2
Enters into or becomes concerned in an arrangement for
Acquisition
Use or
Control
or
If criminal property is retained
S4
Converts
Conceals
Disguises
Transfers
Removes from Gibraltar
S3
Acquires
Uses or
Has Possession of
Discloses that
He or another person has made a report to GFIU, MLRO or Law Enforcement
OR
Investigation is being carried out on him or is being contemplated
Another person is
Engaged in
OR
Attempting to
Money Laundering
This info came about from business, trade, profession, etc
Does not disclose to GFIU
As soon as is practicble
OR
OR
Made an Authorised Disclosure
Has Consent
Intended to make disclosure
Has reasonable excuse
Law enforcement
Acquired property for adequate consideration
If that disclosure is made to;
GFIU,
Police,
Customs, or
Supervisory Body
The person is a notary, independent legal professional, auditor, external accountant or tax advisor
The information obtained from their client;
In the course of ascertaining the legal position, or
Whilst performing the task of defending the client including advice on instituting or avoiding proceedings

MONEY LAUNDERING AND TERRORIST FINANCING

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" means doing any act which constitutes an offence–

(a) under section 2, 3 or 4 of POCA;

(b) doing any act which constitutes an offence under sections 5, 6, 7 or 8 of the Terrorism Act 2005;

(c) doing any act which constitutes an offence under any other enactment that applies in Gibraltar and that offence relates to terrorism or the financing of terrorism,

or in the case of an act done outside Gibraltar would constitute such an offence under that Act if done in Gibraltar.

and

"terrorist financing" means-

(a) 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

(b) the acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes,

and cognate expressions shall be construed accordingly.

PROPERTY AND CRIMINAL PROPERTY

In order to properly understand how the offences work, it is necessary to have an understanding of two very important terms used throughout POCA;

Property

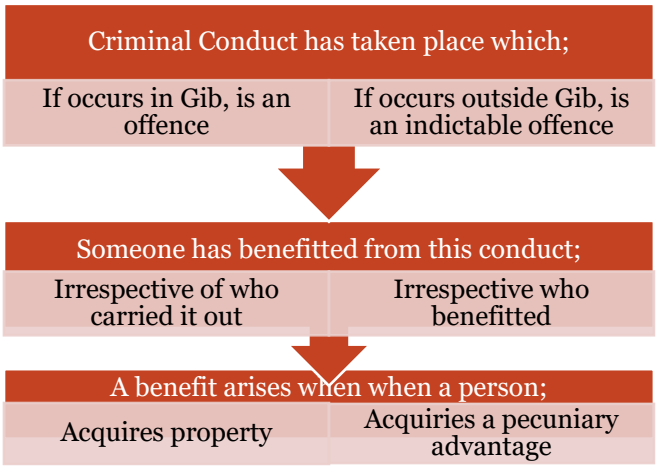
This is defined in S183 and means;

> *"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"*

This definition is drawn from the FATF's current interpretation of the term and it is important to note the inclusion of documents evidencing title or interest in and not just physical assets.

Criminal Property

For a ML offence to take place it must first be established that knowledge or suspicion existed that the property in question was "Criminal Property".



PROHIBITED ACT, THE CONSENT MECHANISM AND THE MORATORIUM PERIOD

If you have a suspicion you are acting in will involve dealing with criminal property, you can make a disclosure to the GFIU via your MLRO and seek consent to undertake the further steps in the transaction which would constitute a money laundering offence

The flowchart on the next page outlines the process in order to proceed with a transaction.

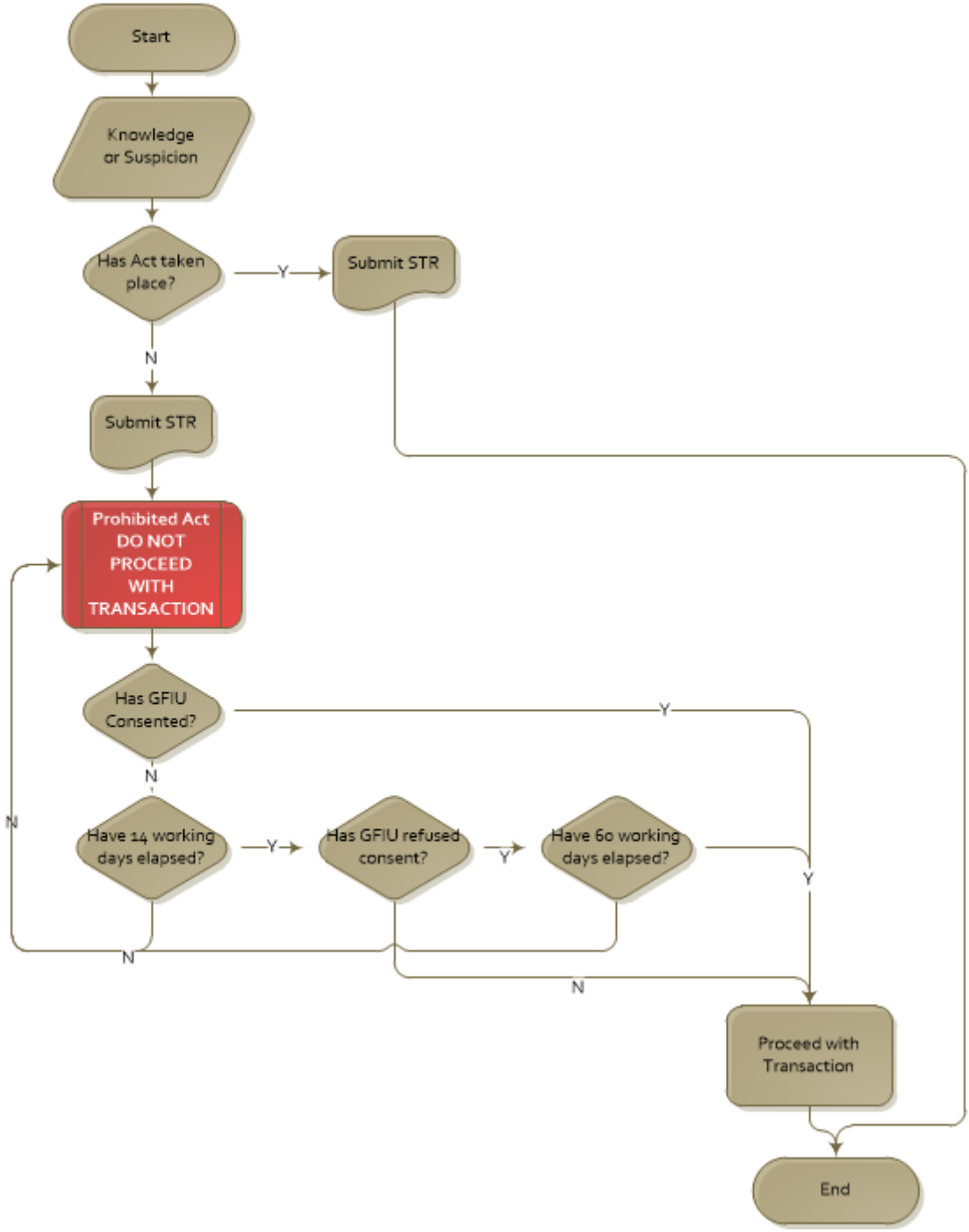


Figure 1 - The Consent Mechanism

It should be noted that negative consent is normally granted by default on the expiration of the 60 working days. This is known as the "moratorium period". The Head of GFIU may, however, apply to the Court to seek an extension of these 60 days for a period of up to 2 years so firms must be certain that no such extension has been sought and granted before proceeding with a transaction.

Suspension of a Transaction

Where there is a suspicion that a transaction is related to Money Laundering, the GFIU may of its own accord make a suspension order to suspend or withhold consent to a transaction that is proceeding. This may occur even in the absence of a STR from a relevant financial business.

Firms who do not comply with the order or who inform the client of the order are guilty of offences under this section.

CHANGES TO PART III – MEASURES TO PREVENT THE USE OF THE FINANCIAL SYSTEM FOR PURPOSES OF ML & TF

A number of important changes to the legislative requirements were made as a result of 4MLD transposition which affects the systems of controls that relevant financial business have to comply with. Most of these requirements were already regulatory requirements imposed by the Financial Services Commission or Gaming Commissioner through their Anti-Money Laundering Guidance Notes (AMLGN).

Relevant Financial Businesses

A number of updates in the definitions of who is covered by the term Relevant Financial Business was necessary to bring our definitions up to date but no new businesses have been caught by the new definitions.

It is understood that there are ambiguities as to the applicability of the requirements to certain types of fund activities and ancillary services. The FSC will be making a submission to the Minster to clarify the applicability of these requirements and if necessary a separate set of Regulations will be published under S9A.

Senior Management Responsibility (S9B, S26A)

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.

"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.

A firm's policies, controls and procedures must not be implemented without the prior approval of senior management (S26A).

Requirement to look through a person (S10A)

Firms must also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

Risk Factors (S11)

On applying a risk-based approach, firms must take into account the following risk variables so it will be important to be able to demonstrate to the regulators that these have been adequately considered and documented;

(a) the purpose of an account or relationship;

(b) the level of assets to be deposited by a customer or the size of transactions undertaken;

(c) the regularity or duration of the business relationship.

Life Assurance Beneficiaries (S13)

Firms dealing in life assurance products must ensure that enhanced CDD is conducted and verification conducted whenever beneficiaries are identified or designated and there is to be a payout.

There are additional controls necessary to determine if such beneficiaries are PEPs.

Low Risk Cases and Simplified Due Diligence Measures (S16)

Firms may apply simplified due diligence measures where it identifies areas of lower risk and has ascertained that the business relationship or the transaction presents a lower degree of risk. However, it must document these considerations carefully and must take into account at least all the risk factors in Schedule 6 of POCA.

High Risk Cases and Enhanced Due Diligence (S17 and S17A)

POCA requires firms who conduct Correspondent Banking or have relationships with PEPs to apply enhanced due diligence measures (EDD). In addition to these, EDD is required when

- when dealing with natural persons or legal entities established in third countries identified by the European Commission as high risk third countries; and
- in other cases of higher risk identified-
    - by the relevant financial business; or
    - by the Minister by notice in the Gazette.

To date the Minister has not published a list of High Risk cases. However, the FSC frequently updated a list of high risk countries as identified by the FATF.

Politically Exposed Persons (S20, S20A, S20B)

The definition of a Politically Exposed Person (PEP) has had a major revision. This now includes domestic PEPs as well as foreign PEPs, which is what used to be caught before.

Firms must ensure that when establishing business relationships, as well as throughout the lifespan of that relationship, they have adequate risk based systems to detect if the proposed or existing customer is or becomes a PEP (S26(2)(c)).

It should be noted that there are new definitions of "Family Members" of PEPS as well as "persons known to be close associates" of PEPs and these persons should be treated as PEPs themselves and subject to the same controls and continuing obligations.

The controls required to operate a relationship or transaction with a PEP have remained largely unchanged.

Firms are advised that in light of the expanded definition of PEPs that processes are put in place to determine if existing customers now fall into this category.

Firms must, for at least 12 months after ceasing to be a PEP, take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.

Branches and Subsidiaries (S21, S26, S28)

Where a relevant financial business operates in other countries, POCA has made it more explicit as to the application of the Gibraltar requirements and requires the termination of relationships where host country standards are not sufficient.

A relevant financial business that has branches or subsidiaries must implement group-wide policies and procedures for sharing information within the group, to the extent permitted under the Data Protection Act 2004.

A group must have in place internal reporting procedures for the purposes of receiving disclosures about knowledge or suspicions of money laundering or terrorist financing that may be taking place with regards to activities related to the group. Information about money laundering and terrorist financing received under this section may be shared between the group unless instructed otherwise by the GFIU.

Third Party Reliance (S23 & S23A)

Firms are now prohibited from relying on eligible introducers from high risk third countries (other than from branches and subsidiaries of EU owned own groups) irrespective if all other criteria is met. Reference to high risk third countries is the list of High Risk Countries published regularly by the FSC.

Risk Assessment (S25A)

POCA requires firms to conduct a formal risk assessment process to identify risks of Money Laundering and Terrorist Financing which must include an assessment of;

- Customers
- Countries or Geographic Areas
- Products
- Services
- Transactions or Delivery Channels
- National Risk Assessment

The risk assessment needs to be documented and kept up to date.

Employee Screening (S26(1)(g), S30(3) & S30C)

A new requirement is that firms must have an employee screening programme 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. (S30(3))

In establishing whether a person is fit and proper to hold a management function or being a beneficial owner of a relevant financial business, the supervisory authorities are now required to conduct criminal checks. (S30C)

Independent Audit Function (S26(1A))

Firms are required to undertake an independent audit which tests the policies, controls and procedures of a relevant financial business on a regular frequency.

Training (S27)

The training requirement for firms has been expanded in POCA which must now also include relevant data protection requirements.

THE GIBRALTAR FINANCIAL INTELLIGENCE UNIT

Those in the regulated sector in particular will have noticed that HMGoG has reassigned existing resources, particularly at HM Customs, to provide GFIU with much needed resources to conduct their statutory functions.

A whole new Part has been inserted into POCA (Part IA) dealing with the establishment and functioning of GFIU as well as providing them it with new powers.

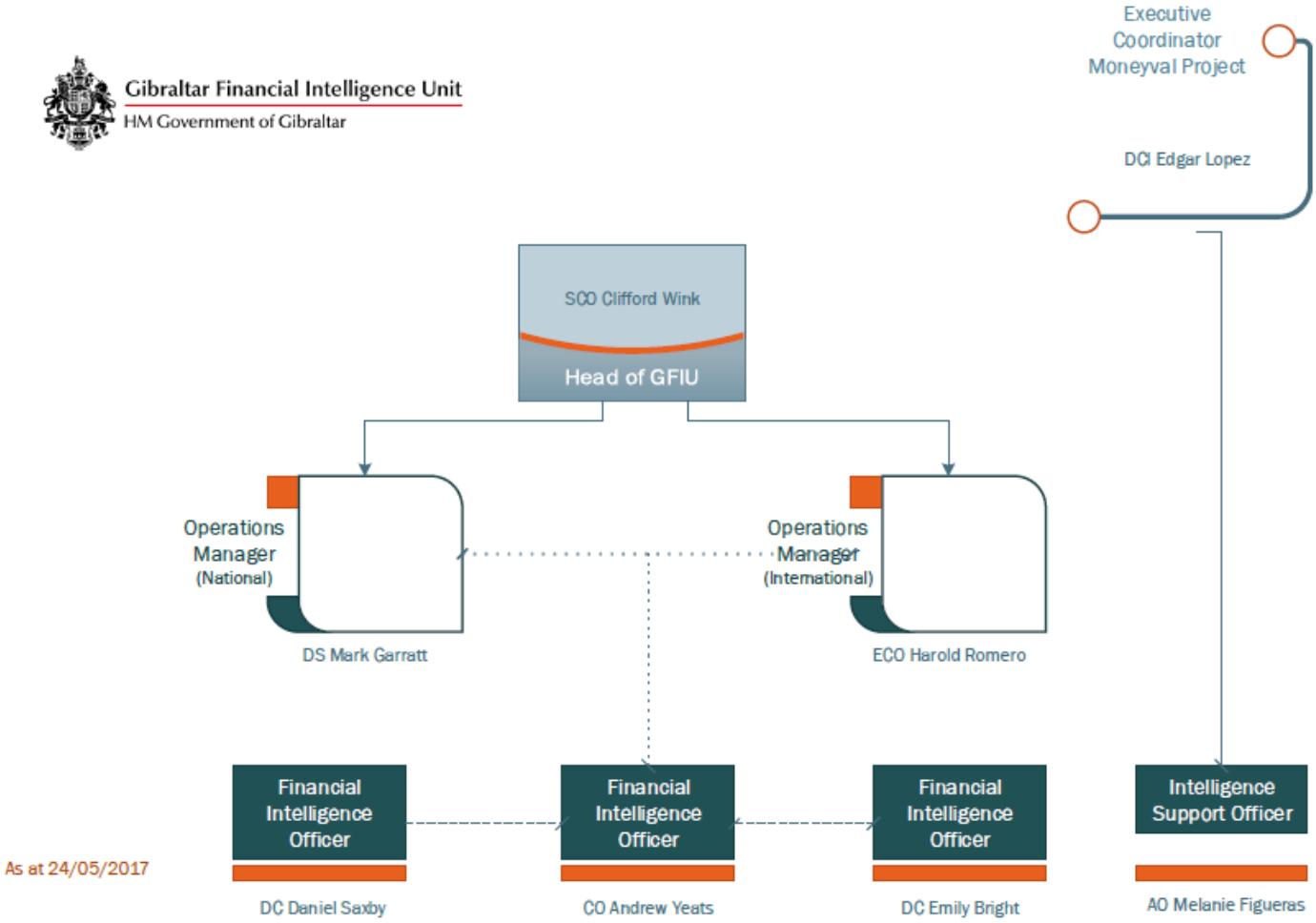
The current set-up and manning of the GFIU is shown in the organisation chart below.

Functions of GFIU

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

GFIU's analysis function shall consist principally of an operational analysis. This will focus on individual cases and specific targets or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use of the information after dissemination and a strategic analysis addressing money laundering and terrorist financing trends and patterns.



Information Gathering Powers (S1ZDA and S1DA)

GFIU has been granted statutory powers in relation to STRs as well as intelligence gathering more generally in order to fulfil its statutory functions. This includes being able to ask for information from relevant financial businesses as well as the financial services regulator, Income Tax Office and Law Enforcement Agencies.

Not assisting the GFIU with the provision of the relevant information is an offence unless a defence (S1DC) applies.

It is important to note that offences in this section can be extended to individuals if it is proven that a corporate body committed this with the consent or contrivance of such individuals.

International Cooperation

There are a number of sections introduced dealing specifically with the provision and seeking of co-operation and sharing of intelligence with other FIUs and the necessary protections required for this.

POWERS OF SUPERVISORY BODIES

Each of the supervisory bodies who have responsibilities for regulating relevant financial business for AML/CFT systems of control have been given identical powers in order to perform their functions. These were introduced by way of secondary legislation in the Supervisory Bodies (Powers Etc) Regulations 2017 (the "Regulations").

Relevant Person

The Regulations apply to all relevant persons and this definition is wider than just the relevant financial business as it includes;

(a) a relevant financial business;
(b) any director, officer or senior manager of a relevant financial business;
(c) any person who is, or who has at any time been, directly or indirectly employed (whether or not under a contract of service) by any of the persons mentioned in paragraphs (a) or (b) above;
(d) any person who has, or who has at any time had, any direct or indirect proprietary, financial or other interest in or connection with any of the persons mentioned in paragraphs (a) or (b) above;
(e) any persons seeking to obtain any direct or indirect proprietary, financial or other interest in connection with any of the persons mention in paragraphs (a) or (b) above;
(f) any person who is, or has been, directly or indirectly involved in a transaction which the relevant supervisory body considers relevant to the pursuit of its obligations under POCA, these paragraphs or any applicable law or guidance.

So, these Regulations may apply to you as an individual as well as the firm for which you work for or have a financial interest in.

Risk Based Approach

The supervisory bodies are required to adopt a risk-based approach to their AML/CFT work which will include both on-site as well off-site elements.

Each firm's risk profile will be reviewed periodically as well as where there are important changes to the business.

International Cooperation

The supervisory bodies are required to provide cooperation with other supervisory bodies and relevant EU bodies.

Powers

The supervisory bodies have been granted general powers to do all things necessary to fulfil their functions including requiring the taking of preventative or corrective actions, information gathering and on-site access.

Information
The Regulations define information very widely;

> *"means any information held by or on behalf of a person including but not limited to, paper records, documents, emails, information stored electronically, audio or video recording devices, microfiche, maps, photographs, handwritten notes or any other form of recorded information and copies thereof"*

Information Gathering
A relevant person can be required to provide information either in person or through the provision of documents etc and copies etc can be taken.

Skilled Persons Report
Supervisory bodies can also require that a report is submitted on a relevant person on any subject. Importantly, the costs of producing such a report is borne by the relevant person themselves.

Inspectors
An inspector may also be appointed by a supervisory body to investigate compliance by a relevant person with their obligations under POCA, any applicable law or guidance.

Duty to produce records, etc.
It is a duty of every person whose affairs are being investigated to provide information in his possession or under his control.

Enforcement and Sanctioning Powers

Default
Generally speaking, the enforcement and sanctioning powers of the supervisory bodies come into effect whenever there is a default. This is defined as;

> *"conduct which has or may lead to a breach of a provision of the Act, these Regulations, or any applicable law or guidance but does not include conduct which constitutes a criminal offence"*

It will be noted that default is both an actual breach or one which may lead to a breach taking place. Also important to note is that if what has occurred has a criminal sanction, these enforcement cannot be pursued.

Penalties
There are severe financial penalty provisions for defaults of POCA, applicable laws or Guidance. These can amount to maximums of;

(a) twice the amount of benefit derived from a default or breach of the applicable law or guidance where that benefit can be determined; or
(b) EUR 1 million;

These penalties can be increased in the case of credit institutions or financial institutions to;

(a) in the case of a legal person-
  (i) EUR 5 million; or
  (ii) 10% of the total annual turnover according to the latest available accounts approved by the management body;
(b) in the case of a natural person, EUR 5 million.

Suspension or withdrawal of licence or authorisation.
A supervisory body may suspend, withdraw or revoke a licence or authorisation where a relevant person has defaulted. Any suspension cannot exceed 18 months.

Temporary ban from managerial positions.
A supervisory body may ban a person from exercising managerial functions in a relevant financial business if that person is responsible for a default or breach of a relevant person's obligations under the Act or any applicable law or guidance. Any suspension cannot exceed 18 months.

Directions
Where a supervisory body;

(a) believes or suspects on reasonable grounds that there is a default or breach of the Act or any applicable law or guidance; or

(b) considers that it is in the public interest to do so,

it may direct the relevant person, at its own expense, to take or refrain from taking any course of action in relation to the fulfilment of its obligations under the Act, these Regulations or any applicable law or guidance that the supervisory body specifies in the notice.

Effective application of sanctions.
In determining the type, duration or level of action to be taken, a supervisory body must take into account all relevant circumstances, including where appropriate-

(a) the gravity and duration of the default or breach;
(b) the degree of responsibility of the responsible person;
(c) the financial strength of the responsible person as indicated-
  (i) in the case of a legal person, by its total turnover; or
  (ii) in the case of a natural person, by his annual income;
(d) the benefit derived from the default or breach by the responsible person, insofar as it can be determined;
(e) the losses to third parties caused by the default or breach, insofar as they can be determined;
(f) the level of cooperation of the responsible person with the supervisory body; and
(g) previous defaults or breaches by the responsible person.

Warning and Decision Notices
Supervisory bodies, before imposing a penalty, suspending or withdrawing a licence, imposing a temporary ban or issuing a direction have to, in addition to considering the above, issue a warning notice of their intention to do so.

This "warning notice" can be waived due to urgency, if it would undermine the effectiveness of the proposed action or if legal proceedings require notice to be given already.

Where a warning notice is issued, the recipient has to be given at least 14 days to make representations and whether these representations may be made orally.

After considering any representations, of if the warning notice has been dispensed with, the supervisory body must do one of the following;

- Confirm the decision and the action that will be taken;
- Discontinue the proposed action in full; or
- Issue a combined notice which contains what actions will be proceeded with and which will not.

A person affected by a decision notice has 21 days in which to launch an appeal and the actions required to be taken in decision notice cannot come into effect until such time as this period has expired.

Alternatively, the supervisory body can state that the actions will not be required to be given effect until the appeal is determined.

The Court may confirm, vary or reverse the matter appealed and may direct the supervisory body to Take any actions which it directs.

Interim Orders
A supervisory body can apply to the Supreme Court for permission to take action where a decision notice has been issued and has not yet taken effect.

Public Statement
Where the decision notice has been issued the supervisory body is obliged by the legislation to make a public statement on its web-site (and keep it there for five years), subject to an assessment of the proportionality of the publication. The statement must state;

- the action taken;
- the type and nature of the default or breach;
- the identity of the person to whom the default of breach is attributed.

If the supervisory body considers that publication is disproportionate or it would jeopardise the stability of financial markets or an on-going investigation it may decide to;

- delay the publication of the statement until the reasons for not publishing it cease to exist;
- publish the statement on an anonymous basis, in a manner which accords with the law, where it is considered that such publication ensures an effective protection of the personal data
- concerned;
- not to publish the statement, where the measures set above would be insufficient to ensure-
    - the stability of financial markets would not be put in jeopardy; or
    - the proportionality of the publication of a statement with regard to actions.

No publication can be made whilst an appeal is pending.

OFFENCES

The Regulations provide for a number of offences and in particular;

- Wilfully making a statement or furnishing information knowing it to be untrue and
- Unwillingness to co-operate.

Where the offence is committed by a body corporate, partnership or unincorporated association an individual can be prosecuted is they contributed by their consent or connivance if the held positions of control or senior management.

CONCLUSIONS

As will be seen from the above there are a number of very important amendments to the operation of the AML/CFT regimes which are important from a preventative and deterrent angle as well as operationally for both Law Enforcement and the private sector.

Further amendments will be required in the months ahead. These amendments will be to ensure that the FATF Recommendations, which are not reflected in the 4MLD transposition, are also given effect. Most of those proposed amendments will be centered around moving current requirements from the AMLGNs into the statute book and providing more clarity as to what is required in order to meet regulators' expectations.

This newsletter has been published by;

The National Coordinator for Anti-Money Laundering and the Combatting of Terrorist Financing
HM Government of Gibraltar
40 Town Range
Gibraltar

August 2017 (Amended 1 Sept 2017)