Gibraltar Financial Intelligence Unit
HM Government of Gibraltar

Guidance Notes for Submission of Suspicious Activity Reports

MLRO & Reporters

01 October 2020

Version 1.0

Table of Contents

Scope

This guidance is produced by the Gibraltar Financial Intelligence Unit (GFIU).[1]

The GFIU has responsibility for receiving, analysing and disseminating financial intelligence submitted through the Suspicious Activity Reports (SARs) regime. GFIU works with law enforcement agencies, government agencies, supervisory bodies and currently over 160 other international Financial Intelligence Units (FIUs) to prevent and disrupt money laundering and to counter the financing of terrorism.

The content of this document contains information that will assist Money Laundering Reporting Officers (MLROs) and/or Nominated Officers, referred to collectively as 'Reporters' in this guidance. It is general in nature so you should always also refer to the relevant, up-to-date legislation. If any errors are discovered, please inform the GFIU. Please note that the relevant competent authority in Gibraltar would consider each matter on the facts, and the specific legal requirements that apply. Neither the GFIU nor the Gibraltar competent authorities can issue definitive guidance on how the law might be applied in a particular case or how a Gibraltar court might interpret the law. **Finally, this guidance does not represent legal advice. If you are unsure about your obligations in a given case, you should take independent legal advice**.

1 Introduction to Suspicious Activity Reports

1.1 The Suspicious Activity Report (SAR)

This is a report submitted to the GFIU with information which alerts law enforcement that certain client/customer or related business activity is in some way suspicious and might indicate money laundering or financing of terrorism. Also known as a 'disclosure', and can refer to any information acquired by the Reporter in the course of business deemed suspicious and of potential interest to Law Enforcement Agencies. Another recognised form of referring to a SAR is 'STR' (Suspicious Transaction Report) but GFIU will refer to it as a SAR throughout this document. Throughout this document the term '*disclosure*' and 'SAR' are used interchangeably but both have the same meaning.

1.2 Reason for Submitting a SAR

Submitting a SAR provides law enforcement with valuable information on potential criminality, which can lead to the instigation of new investigations or enhance on-going operations. It also protects you, your organisation and Gibraltar financial institutions from the risk of laundering the proceeds of crime. By submitting a SAR to the GFIU, you will be complying with any potential obligations you have under the Proceeds of Crime Act 2015 (POCA) and the Terrorism Act 2018 (TACT).

1.3 Suspicion Under POCA

Suspicion is not defined in legislation and depends on many factors. It is a personal, subjective and objective test, falling far short of proof based on firm evidence. It is a concept that will vary depending on the circumstances in which it is applied as various factors must be weighed up by the Reporter.

[1] This document contains information extracted from the UKFIU's guidelines which have been included with their kind permission.

Suspicion would fall below knowing something to be true (needing proof or firm evidence), be thought of as being something that can be reasonably inferred from the circumstances (common sense or measuring against the norm) and, must be more than just mere speculation (unreasonable or irrational – jumping to conclusions).

The risk assessment that is performed on the client, is an important factor. The more knowledge and experience the Reporter has will also assist in formulating suspicion. There must exist, as a minimum, an aspect of the transaction or activity that the Reporter feels is at odds and does not conform to normal expectations, be it through inference, sight of documents, client´s comments, professional insight or based on the foundation that the Reporter believes something is not quite right. It is more than just a feeling. The Reporter must judge if a possibility exists even if he does not have the specific facts to support it.

This reasoning is sufficient and now means a reporting obligation exists as a reasonable doubt as to the origin of the assets or the nature of the transaction or activity.

However, it must be more than just speculation. A reasonable doubt should exist. The threshold for a transaction or activity to be 'suspicious' is low. Definite knowledge, proof or evidence of the fact is not required to raise a SAR.

The GFIU, will not comment upon what circumstances should or should not be deemed suspicious.

1.4 Suspicious Transaction or Activity

Suspicious activity or transaction usually relates to where money laundering or financing of terrorism is possibly involved. The sum of money involved in the transaction is irrelevant. There is no monetary threshold for making a report of a suspicious transaction.

For example;

- Transactions with individuals, corporate persons and financial institutions in or from other countries which do not, or insufficiently comply with established regulatory or other financial requirements;
- Transactions which are complex, unusual or large (whether completed or attempted);
- unusual patterns of transactions;
- periodic transactions which have no apparent or visible lawful purpose;
- the receiving or making of a gift;
- a one-off transaction. This means any transaction other than one carried out in the course of an existing business relationship;
- two or more one-off transactions which appear to be linked;
- the customer activity deviates from the normal activity for that customer, business or sector.

The Reporter should consider and understand what is the normal activity or business practice for each customer or client and establish where or how the suspected

transaction or activity differs from that. The Reporter should consider all the circumstances of the transaction and include consideration of the knowledge of the client's/customer's business, their financial history, background and behaviour. Some factors may seem individually insignificant, but taken together may raise the suspicion of money laundering or the financing of terrorism.

Any transaction/activity that causes a Reporter to have a feeling of apprehension or mistrust about the transaction should be closely examined and the Reporter should consider submitting a SAR.

1.5 Identifying Suspicious Transactions or Activities

There are a number of general indicators that can be used, known as 'red flags,' that are helpful in identifying a suspicious transaction/activity. The presence of one or more of these indicators does not necessarily mean that money laundering or financing of terrorism is in fact taking place, but is useful in providing enough of an indication for the Reporter to pay close attention to the matter. The Reporter must reach his conclusions upon examining the transaction or activity both subjectively and objectively, and give careful consideration to the circumstances, conditions and evidence before him.

Red flags which point to a transaction being related to the financing of terrorism are similar to those relating to money laundering and it is possible that a transaction or activity could be related to both. For example, funds used for terrorist activity could be the proceeds of criminal activity as well as from legitimate sources.

2 Submitting a Suspicious Activity Report

A good SAR narrative should contain enough information that the GFIU can use to make informed decisions for analysis and further dissemination to law enforcement agencies, supervisory bodies or other public sector body. The content of the narrative and the supporting documentation are vital to the process of linking investigations and ultimately lead to a criminal prosecution.

As a basic guide, wherever you can, try to answer the following six basic questions to make the SAR as useful as possible:

Who? What? Where? When? Why? How?

Who is conducting the suspicious activity?

Provide as much information as possible that you have on the subject. If any other subjects or entities are involved or connected they should also be added to the SAR.

What is suspicious about the activity?

Provide the information available on the instruments, services or mechanisms that were used to enable the suspicious activity. For example, shell companies, ATMs, wire transfers, virtual asset wallet address and/ or source of funds.

When was the suspicious activity identified?

Providing a description of the suspicious activity in a chronological order will assist the reader in understanding the report better. Include over what period of time the suspicious activity occurred and whether there are any previous SARs that are linked to this activity or subject.

Where did the suspicious activity occur?

Provide the information of the location of the suspicious activity and any other location or jurisdiction impacted by this activity.

Why is the activity suspicious?

Provide reasons as to why the activity is considered suspicious and what is unusual for the subject, services offered by the reporting entity, or any inconsistency with the subject's financial history and risk profile.

How was the suspicious activity executed?

Provide information on how the activity occurred, if it was a one off transaction or a series of transactions. Including the source of funds will assist investigators.

2.1 When to Submit a SAR

As soon as you '**know**' or '**suspect**' that a person (or other entity) is engaged in money laundering or dealing in criminal property, you must submit a SAR as soon as is practicable. Time may be of the essence, especially if the SAR is going to be accompanied

by a Consent request (see Consent or DAML below in Section 4). Reporters will need to strike a balance between the timely submission to the GFIU and the need to obtain all the relevant information required by the GFIU to make an informed decision. Therefore, Reporters should ensure their internal systems support the timely submission of SARs and unnecessary delays should be avoided. Any suspicious activity or transaction related to the Financing of Terrorism should be submitted immediately and followed with additional information once obtained.

2.2 Reporting Obligations

The reporting obligations in POCA are applicable to anyone in Gibraltar that may interact with an individual or business, whereby they may commit a money laundering offence.

Those working in the 'regulated sector' commit an offence if they do not submit a SAR to the GFIU if they know or suspect, or have reasonable grounds to know or suspect, that another individual or person is engaged in money laundering; and the information came to them in the course of their business in the regulated sector (Section 6B POCA).

Those reporting to the GFIU need to be aware of the "tipping off provisions" which make it an offence, having submitted a SAR to reveal information which is likely to prejudice any resulting law enforcement investigation.

2.3 Reporting via THEMIS

THEMIS is now the preferred and recommended method for the reporting of activity suspected to be associated with money laundering or financing of terrorism. Reporting entities with money laundering or financing of terrorism reporting obligations under POCA and TACT will be requested to register their Money Laundering Reporting Officers (MLROs), nominated persons or other with GFIU so that access can be authorised. THEMIS not only provides a secure means for the submission of SARs and other financial intelligence to the GFIU but it also allows the GFIU to communicate important information to Reporters.

SARs may be reported as follows:

- Via THEMIS, the GFIU's secure online reporting system on https://www.disclosures.gov.gi
- In urgent cases a report may be made by phone to (+350) 200 70211, prior to submitting;
- Out of Hours (Urgent calls only e.g. Terrorist Financing): (+350) 56346000;
- As otherwise agreed with the GFIU prior to reporting.

Where there are particular sensitivities or concerns about submitting a SAR, the GFIU should be contacted on (+350) 200 70211.

Priority must be given to making an immediate report (verbal or otherwise) if the Reporter;

- understands that there exists a transaction or activity that has gone beyond suspicion and that there is knowledge or belief that money laundering or financing of terrorism is occurring;
- believes a crime is imminent;

- thinks there is a risk of transfer/ withdrawal/ conversion of funds/ assets out of the jurisdiction which may be irrecoverable.

2.4 Failing to Report

Even if you are not in the regulated sector, you may have an obligation to submit a SAR. You may commit an offence if, you have 'knowledge' or 'suspicion' of money laundering activity or criminal property; do something to assist another in dealing with it, and fail to make a SAR.

2.5 No Access to THEMIS

Any person wishing to submit a SAR to the GFIU and does not have access to THEMIS may do so by either contacting the GFIU on (+350) 200 70211 or by submitting a manual SAR that is available for download from the GFIU website (https://www.gfiu.gov.gi/reporting).

2.6 Anonymous Reporting

Any person may submit a SAR to the GFIU. As soon as a SAR is received by the GFIU it will be entered into THEMIS which provides a secure platform for all financial intelligence held by GFIU. Should you wish to submit a SAR anonymously you can do so by downloading it from the GFIU website (https://www.gfiu.gov.gi/reporting) and submitting it via post to the following address:

Gibraltar Financial Intelligence Unit

Suite 945

Europort

GX11 1AA

Gibraltar

2.7 Confidentiality of the SAR Data

All GFIU officers adhere to specific guidelines including to protect the confidentiality of SARs. Once a SAR is received by the GFIU, it is held on THEMIS, a secure platform.

THE INFORMATION IS ALWAYS HELD IN THE STRICTEST CONFIDENCE

If, in the unlikely event you are made aware that any confidentiality may have been breached, you should contact the GFIU immediately.

3 Submitting Better Quality SARs

The introduction of THEMIS in January 2019, has seen a general improvement in the quality of SARs submitted. THEMIS contains a larger number of fields that Reporters can follow as a guide to enter data required by the GFIU. Completing all the required fields and including as much detail in the narrative will ensure that there is enough information on which the GFIU can make informed decisions. It will also reduce the amount of time spent between the GFIU and the Reporter in obtaining further information that may be have been lacking. This section is designed to assist Reporters in making improvements to the quality of the data and information provided.

3.1 Producing a Quality Report

Producing a quality report gives Law Enforcement Agencies the context it requires to make better judgements and to be able to investigate the suspicion raised by a Reporter.

The quality of the information within the SAR is important and the GFIU recommends that you structure the narrative of your SAR in a logical format including all relevant information:

- Briefly summarise your suspicion.
- Provide a chronological sequence of events. Keep the content clear, concise and simple.
- Avoid acronyms and jargon – they may not be understood by the recipient and are open to misinterpretation. If describing a service provided or a technical aspect of your work, please provide a brief synopsis in your SAR to aid the reader.
- If including a large amount of information/text, break it up into more manageable – and readable – paragraphs.
- Very long SARs that are text heavy are difficult to digest.
- Use punctuation.
- Whenever possible, scanned attachments should be in an OCR format.
- Previous SAR reference if the subject has been the subject of a SAR.

3.2 Grounds for Suspicion

The SAR narrative is essential to determine the reasons for the suspicion. It should contain a detailed explanation of the reason for the knowledge or suspicion that has triggered a SAR. The content of the suspicion must be written with sufficient information that a reader with no prior knowledge of the activities is able to understand the reasons for suspicion. The Reporter should also include when the suspicious activity occurred including the date it was first identified as well as the period of time over which the activity has been observed.

It is also important that the Reporter clearly explains the rationale for submitting the SAR. It is good practice to include why the activity or transaction is suspicious for the client/ customer, providing an account of normal expected activity of other clients/ customers. Being aware of a criminal 'modus operandi' for the products or services provided by your company or reporting sector will assist you in formulating the suspicion.

3.3 Subject(s)

The subject(s) in a SAR is very important to the GFIU to be able to conduct further enquiries and to eliminate potential matches. If certain information is not known at the time of submitting the SAR it should be explained in the SAR. All the fields that identify the subject should be provided in their respective fields within THEMIS. These include the following:

- Full name (ensuring that care is taken with spellings)
- Other Names (e.g. former name, aliases)
- Date of Birth
- Nationality
- Gender
- Occupation (include their business email/ telephone number)
- Addresses (include residential address, all other known addresses)
- Identification details (e.g. passport, ID card, driving licence)
- Whether a PEP/MEP

For Entities (name/ other names, e.g. former name, business name, etc.)

- Registration Number
- Date of Incorporation
- Place of Incorporation
- Business Addresses
- Business email/ telephone number and if available the business website
- Officers (e.g. directors, shareholders, beneficial owners, etc.)

3.4 Transactions

The Reporter should clearly identify the methods by which the suspicious activity is being conducted. This includes whether the suspicion relates to financial transactions. The information should include the type of transaction and the details and role of the sender/ receiver of the funds (e.g. depositor). Information that appertains to the transactions, e.g. account number, sort code, IBAN etc. The GFIU would recommend that in cases where there are numerous transactions that these are uploaded in THEMIS as attachments in the appropriate file format (e.g. CSV).

3.5 Further Information

Disclosures may require additional information to be added in the form of supporting documentation. This can be done via THEMIS. When further information is received or obtained by the Reporter, it can also be either uploaded on THEMIS or written as free text in the 'Further Information' tab. Updates can also be provided to the GFIU even after the submission of the disclosure.

3.6 Dual Reporting

Some SARs may be required to be submitted to an FIU in another jurisdiction. THEMIS provides a field for a reference number provided by the foreign FIU. In cases where there is no reference number then this information should be included in the 'Summary' field so that the GFIU can refer to the report if required.

Reporters are reminded that Section 1G (2) of POCA, requires a reporter to transmit the information it sends to the GFIU in relation to a disclosure to the relevant EU FIU where the relevant financial business is established in a Member State.

3.7 Dual Reporting Gambling Sector

Dual reporting is common within the Gambling sector. A dual reporting arrangement was made between Gibraltar and the UK to ensure a consistent approach amongst operators.

As per UKGC guidelines, SARs concerning British customers resident in the UK (where consent/ Defence Against Money Laundering [DAML] is being sought) a disclosure is to be submitted to the UKFIU for the purpose of seeking the relevant consent or otherwise as the case may be.

These 'consent' (DAML) SARs shall be dually reported but will first be sent to the UKFIU and then to the GFIU once it has been notified that consent has been granted or not (including when no response is received after the 7th day – i.e. implied consent). Consent matters will be actioned by gambling operators accordingly as directed by the UKFIU. When reporting to the GFIU, operators will be asked to provide the UKFIU's URN and the UKFIU's response if available. All non-consent SARs concerning British customers will continue to be submitted to the UKFIU with the dual report to the GFIU as required by POCA 2015.

When a DAML has been requested from the UKFIU there is no requirement to complete a DAML request to the GFIU. Reporters are to note that the THEMIS 'consent' tab should not be used to provide that information to the GFIU. It should be contained within the narrative of the SAR. Using 'consent' tab for this will automatically trigger an alert to the GFIU and valuable resources are unnecessarily diverted.

3.8 Requests for Additional Information from GFIU

The GFIU may require Reporters to provide further, additional information or clarification to a SAR submitted. This will be done via THEMIS and the response should also be provided by updating the SAR. There is no requirement to submit a separate SAR.

3.9 Timeliness of Responding to requests from GFIU

When the GFIU make a request for additional information the Reporter must provide the GFIU with such additional information relating to that SAR and must do so within a reasonable period as the GFIU may require.

4 Consent – Defence Against Money Laundering

The GFIU has reviewed the term 'consent' and has determined that in order to improve the understanding of the term it has adopted the use of the term Defence Against Money Laundering or Defence Against Terrorist Financing (DATF). This terminology reflects more accurately the intention behind the legislative provisions and is expected to improve the quality of the requests received by the GFIU. It must be noted that the term consent is a legal term and will therefore continue to be used in formal letters and responses issued by the GFIU.

This section provides an overview of consent, for more detailed information you should always refer to the up-to-date version of the legislation.

4.1 Seeking Consent or a Defence Against Money Laundering (DAML)

Persons and businesses generally, and not just those in the regulated sectors, may avail themselves of a DAML charges. This can be done by a consent, via THEMIS, together with the relevant SAR. This consent is to conduct a transaction or undertake an activity about which they have concerns. The legislation gives the GFIU fourteen (14) working days to respond to the consent request. Where the GFIU refuses consent, the transaction or activity must not proceed for a further sixty (60) working days, unless notified by the GFIU of its consent. It must be noted that the 60 working days does not apply to a DATF. Once consent is requested through THEMIS, it provides three options to the GFIU;

- Consent Granted
- Consent Refused
- Not Applicable

4.1.1 Consent Granted

When Consent is granted, the GFIU will inform the Reporter via THEMIS within the 14 working days after the disclosure is made and the reporting entity may process the transaction or activity subject to business considerations. This means that the individual handling the transaction or carrying out the activity, or the Reporter, will have obtained a DAML charges in respect of that transaction or activity it proceeds.

A granted response from the GFIU does not:

- imply GFIU approval of the proposed act(s), persons, corporate entities or circumstances contained within the disclosure;
- oblige or mandate a Reporter to undertake the proposed act;
- provide derogation from, or replace, a Reporter's professional duties of conduct or regulatory requirements, such as for example, those concerning customer due diligence;
- provide a Reporter with a criminal defence against other criminal offences pertaining to the proposed act, or
- override the private law rights of any person who may be entitled to the property specified in the disclosure.

In the event that GFIU does not give notice that Consent is refused within the 14 working day period, it can be taken as 'implied consent'.

4.1.2 Consent Refused

When Consent is refused, the GFIU will inform the Reporter via THEMIS and a restraint order must be obtained by the authorities within a further 60 working days (the moratorium period) from the day the request is refused, if they wish to prevent the transaction going ahead after that date. The court may, on an application by the authorities, grant an extension of a moratorium period.

4.1.3 Not Applicable

A Consent request may not meet the legal requirements or may not contain enough information for the GFIU to consider it. In these circumstances, the GFIU may respond with a 'not applicable' letter. The letter will outline the reason why the request was not applicable under the consent regime. However, reporting officers should note that if the suspicion remains, that there is still a legal obligation to make a disclosure before the 'prohibited act' takes place and should obtain the appropriate consent.

4.2 How to Seek Consent or a Defence Against Money Laundering (DAML)

Reporters wishing to seek consent or a DAML must do so via the THEMIS portal under the *Consent* tab.

A DAML can also be requested after the SAR is submitted with no requirement to create a new SAR.

For more detailed information on requesting consent via THEMIS please refer to the THEMIS user manual.

It is advisable that the following information is included in the request:

- a description of the property that you know, suspect or believe is criminal property; and
- a description of the prohibited act for which you seek a defence.

Some examples of common prohibited acts include:

> "We seek a defence to transfer the closing balance of £3,000 of the client's account to their alternative account at The Rock Bank, Sort Code 00-11-22, Account Number 012345678."

> "We seek a defence to exchange contracts, complete the property purchase, and transfer the sale proceeds to the client's account at The Rock Bank, Sort Code 00-11-22, Account Number 012345678."

> "We seek a defence to retain £1,800 held in the client's account at The Rock Bank, Sort Code 00-11-22, Account Number 012345678."

5 Offences

Gibraltar's anti money laundering and counter terrorist financing framework consists of legislation and industry guidance, in accordance with Financial Action Task Force (FATF) international standards and European Union (EU) Directives.

POCA consolidated, updated and reformed previous local legislation relating to money laundering and criminal property. POCA criminalises all forms of money laundering and creates offences concerning failure to report suspicion of money laundering.

5.1 Money Laundering Under POCA 2015

The three principal money laundering offences are contained in Part II, sections 2, 3 and 4 of POCA. These offences are punishable by a maximum of 14 years imprisonment and/or a fine.

The offences are:

Section 2

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.

Section 3

A person commits an offence if he acquires, uses and/or has possession of criminal property.

Section 4

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

In addition, ***Section 5*** *refers to the offence of Tipping Off and is punishable by a maximum of 5 years imprisonment and/or a fine*.

5.2 Terrorist Financing Under TACT 2018

The terrorist financing offences in the Act are broken down into the following;

Section 35 - Raising funds for terrorism.

A person commits an offence if he:

- Invites another to provide money or other property and intends that it should be used, or has reasonable cause to suspect that it may be used, in full or in part, for the purposes of terrorism.
- Receives money or other property intends that it should be used, or has reasonable cause to suspect that it may be used, in full or in part, for the purposes of terrorism.
- Provides money or other property and knows or has reasonable cause to suspect that it will or may be used, in full or in part, for the purposes of terrorism.

Section 36 - Use and possession of money or other property for terrorism.

A person commits an offence if he:

- Uses money or other property for the purposes of terrorism.

- Possesses money or other property and intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

Section 37 - Arranging funds for terrorism.

A person commits an offence if he enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to be made available to another and knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

Section 38 - Insurance against payments made in response to terrorist demands.

An insurer under an insurance contract commits an offence if

- the insurer makes a payment under the contract, or purportedly under it;
- the payment is made in respect of any money or other property that has been, or is to be, handed over in response to a demand made wholly or partly for the purposes of terrorism; and
- the insurer or the person authorising the payment on the insurer's behalf knows or has reasonable cause to suspect that the money or other property has been, or is to be, handed over in response to such a demand.

Section 39 - Money Laundering.

A person commits an offence if he enters into or becomes concerned in an arrangement of terrorist property:

- by concealment;
- by removal from the jurisdiction;
- by transfer to nominees; or
- in any other way, which facilitates the retention or control by or on behalf of another person of such property.

5.3 Criminal Conduct and Criminal Property

Criminal conduct and criminal property are defined in Section 182 of POCA.

The legislation covers all criminal property, where the alleged offender knows or suspects the property constitutes or represents benefit, being property or a pecuniary advantage, as a result of or in connection with any criminal conduct.

Criminal conduct is conduct which –

- if it occurs in Gibraltar must constitute an offence in Gibraltar; or
- if it does not occur in Gibraltar would constitute an indictable offence in Gibraltar if it had occurred in Gibraltar.

Property is defined in Section 183 of POCA.

Property means any asset situated anywhere in the world e.g.

- Corporal or incorporeal;
- Moveable or immovable;
- Tangible or intangible;
- Legal documents or instruments in any form evidencing title or an interest;
- An interest in property including any equitable interest or right.

5.4 Terrorist Property

It is important to note that the TACT refers to "property" in many instances and it is worth noting the definition in Section 2 of the Act which is;

"property" is to be construed widely and includes property of any description including-

- assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;
- not only such property as has been originally in the possession of or under the control of any person but also any property into or for which the same has been converted or 3 exchanged, and anything acquired by such conversion or exchange whether immediately or otherwise".

5.5 Tipping Off

This is covered by Section 5 POCA and the offence is made out if a person discloses to another that:

- a disclosure has been made under POCA, e.g. a SAR; or
- an investigation is being contemplated or being carried out into
    - a money laundering offence;
    - an offence of tipping off; or
    - an offence of failure to disclose a suspicion or money laundering.