Gibraltar Financial Intelligence Unit
HM Government of Gibraltar

Law Enforcement Investigatory Powers to Aid Financial Investigations into Money Laundering and Other Criminal Conduct

Guidance Notes

March 2022

Table of Contents

Introduction and Scope

The prevention of the use of the financial system for the purposes of money laundering, terrorist financing and other criminal conduct is indispensable to the collaborative effort between the Gibraltar Financial Intelligence Unit (GFIU) and other law enforcement agencies, government agencies, supervisory bodies and over 160 other international Financial Intelligence Units (FIUs) to prevent and disrupt money laundering and terrorist financing.

This note explains the various circumstances in which institutions identified as most vulnerable to the risk of being used for money laundering or terrorist financing purposes may be required to provide law enforcement agencies and other organisations with financial information about their customers under the *Proceeds of Crime Act 2015* (POCA) and other legislation.

This Guidance Note is divided into two parts.

Part 1 - provides guidance on the statutory provisions and circumstances under which the GFIU can request customer financial information from firms.
Part 2 - provides guidance on the statutory provisions and circumstances under which other Gibraltar law enforcement agencies may request such information.

This Guidance Note should be read in conjunction with guidance on the GFIU website www.gfiu.gov.gi.

Please note that 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 the courts might interpret the law. Please also note that the relevant competent authorities in Gibraltar would consider each matter on the facts and the specific legal requirements that apply.

This guidance is not intended to be, and should not be relied on as legal advice. The GFIU strongly advises you to refer to the relevant, up-to-date legislation. If you are

unsure about your obligations, you are strongly encouraged to obtain independent legal advice. This guidance may be updated from time to time. Always check that you are referring to the latest version.

What is money laundering?

For the purposes of Part III of the Proceeds of Crime Act 2015 which creates measures to prevent the use of the financial system for the purposes of money laundering, terrorist financing and proliferation financing *money laundering* means doing any act which constitutes an offence–

- under section 2, 3 or 4 of the Proceeds of Crime Act;
- under section 35, 36, 37, 38A or 39 of the Terrorism Act 2018;
- 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

  (section 7(2) POCA).

Information requests and data protection

Intuitions and professionals often owe their clients a duty of confidentiality, and certain other protections with respect to use and processing of their personal data pursuant to the joint operation of the Gibraltar GDPR (EU regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[1]) and the Data Protection Act 2004 (rules of the GDPR). However, these obligations are not absolute. The Data Protection Act 2004 makes provision for the exemption from, and adaptations of the application of, rules of the GDPR in a number of circumstances.

Part 1 of Schedule 2 of the Data Protection Act 2004 adapts and restricts the application of various data protection principles and data subject rights for the processing of personal data for the purpose of the prevention or detection of a crime in circumstances where the application of such data subject rights (such as the duty to be informed of the processing of personal data) would be likely to prejudice:

[1] As it forms part of Gibraltar law by virtue of section 6 of the European Union (Withdrawal) Act 2019.

(a) the prevention or detection of a crime;

(b) the apprehension or prosecution of offenders; or

(c) the assessment or collection of a tax or duty or an imposition of a similar nature.

The restriction of the application of the Gibraltar GDPR data protection principles and subject rights in such circumstances, in effect, means that provided that there is a lawful compulsion (such as those discussed in this guidance note) to provide the requested information (the lawful requirement being a Gibraltar GDPR principle that is not excluded), entities can provide their customer's personal data to law enforcement agencies for use in investigations into suspected money laundering and other offences without fear of breaching the Gibraltar GDPR or Data Protection Act 2004. Institutions should always refer to their appointed Data Protection Officers for assistance in understanding their data protection obligations.

PART 1 – GFIU Information requests

1 GFIU requests for financial information – The Proceeds of Crime Act 2015

1.1 Introduction - The Proceeds of Crime Act 2015

The Proceeds of Crime Act 2015 is the principal legislative instrument by which Gibraltar has transposed the provisions of the Fourth Money Laundering Directive ((EU) 2015/849) and the Fifth Money Laundering Directive ((EU) 2018/843) into domestic law and ensures that its anti-money laundering and terrorist financing regime (AML/TF regime) is aligned with Financial Action Task Force (FATF) international standards and recommendations. It creates obligations on firms to assist the GFIU in the fulfilment of its functions and other law enforcement agencies, such as the police and customs with their investigations into suspected money laundering and other offences, by providing them with client financial information.

1.2 Information requests by the GFIU

The GFIU is tasked with the collection, analysis, maintenance and dissemination of intelligence related to criminal conduct transacted or attempted to be transacted through relevant financial businesses. In addition to customer due diligence and suspicious activity reporting obligations pursuant to Part III of POCA (see Guidance Notes for Submission of Suspicious Activity Reports for more information), firms working in the finance sector or related industries, within the meaning of "relevant financial businesses" (see definition below at section 1.4.3.1) may be required to respond to GFIU information requests pursuant to the provisions of Part I of the Proceeds of Crime Act.

The Proceeds of Crime Act provides the GFIU with a number of information gathering powers including the power to request financial information from firms where a firm has not submitted a suspicious activity report. Recital 17 to Fifth Money Laundering Directive explains that financial intelligence units' unfettered access to information is essential to ensure that flows of money can be properly traced and illicit networks and flows can be detected at an early stage.

The four separate circumstances when the GFIU may request information held by financial institutions under POCA are:	
Section 1DZA	Requests following a disclosure to the GFIU.
Section 1DA	Requests in response to GFIU disclosures from other persons.
Section 1DAA	Requests in fulfilment of any of the GFIU's functions
Section 1GA	Following requests from other FIUs.

1.3 Requests following disclosure to the GFIU – Section 1ZDA

When any person makes a report to the GFIU such as a disclosure or SAR in accordance with the Proceeds of Crime Act or any other enactment, the GFIU may request additional information relating to that disclosure (s.1ZDA POCA).

Such requests will usually be made via THEMIS (online reporting system) and will provide a time frame for compliance, but the GFIU may request further information in another form. For more information, when and how to make a disclosure to the GFIU and the use of THEMIS see Guidance Notes for Submission of Suspicious Activity Reports.

1.4 Requests in response to GFIU disclosures from third parties and requests in the fulfilment of the GFIU's functions

1.4.1 Requests in response to GFIU disclosures from other persons – Section 1DA

The Proceeds of Crime Act provides the GFIU with further information gathering powers in response to reports received by the following persons (reporters):

- a relevant person (defined below);
- the Financial Services Commission;
- a financial intelligence Unit (FIU) outside Gibraltar;
- the Commissioner for Income Tax;
- a police officer; or
- customs officer.

When the GFIU receives a disclosure from any of the above-mentioned reporters and reasonably considers that, for the fulfilment of any of its functions, it is necessary or expedient to seek additional information from a *relevant person* (not the reporter) who is either:

- mentioned or otherwise identifiable from the disclosure; or
- to the reasonable belief or knowledge of the GFIU, holds information that is relevant to the analysis of the disclosure;

the GFIU may make a request to the *relevant person* for the provision of additional information (s. 1DA POCA) and upon receipt of such a request, the relevant person must provide the additional information in the form and by the date or reasonable period that the GFIU requires.

1.4.2 Requests in fulfilment of any GFIU function – Section 1DAA

If the GFIU has reasonable knowledge or belief that a *relevant person* holds information that is relevant to the fulfilment of <u>any</u> of the GFIU's functions, it may, if it considers it necessary or expedient, make a request for that information from such a *relevant person* who upon receipt of such a request, must provide the information in such form and by such date as the GFIU may require (s.1DAA POCA).

The main functions of the GFIU are–

- to gather, store, analyse and disseminate intelligence related to criminal conduct, (including but not limited to money laundering, terrorist financing and proliferation financing), transacted or attempted to be transacted through relevant financial businesses;
- to act as the recipient for disclosures of suspicious transactions under the relevant applicable legislation;

- to exchange information regarding criminal conduct with FIUs and other similar bodies and law enforcement agencies within and outside of Gibraltar; and
- to consent or deny consent to suspicious transactions of which it has been notified, in accordance with section 4A and section 4B POCA.

(s. 1C POCA).

1.4.3 Who is a *relevant person*?

The GFIU can exercise its s.1DA and s.1DAA investigatory powers to request information from any "*relevant person*". For the purposes of the exercise of these investigatory powers "*relevant person*" means a person carrying on a "*relevant financial business*" within the meaning of section 9 POCA.

1.4.3.1 What is "*relevant financial business*"?

A "*relevant financial business*" within the meaning of section 9 POCA is any person in the business of engaging in one, or more of the following businesses or activities:
• electronic money issuing or deposit taking business carried on by a person who for the time being an authorised institution under the Financial Services (Banking) Act;
• business of the Saving Bank or the Gibraltar International Bank
• any home regulated activities carried on by European institutions;
• investment business within the meaning of the Financial Services (Investment and Fiduciary Services) Act;
• any of the activities in points 1 to 12 or 14 of the Annex I to the Consolidated Banking Directive other than an activity falling within paragraphs (a) to (e);

- insurance business carried on by a person who has received official authorisation pursuant to Article 6 or 27 of the First Life Directive;

- auditors, insolvency practitioners, external accountants and tax advisors;

- estate agents and letting agents;

- art market participants;

- art storage freeport operators;

- notaries and other independent legal professions, when they participate whether-
    - by assisting in the planning or executions of transactions for their client concerning the –
        - buying and selling of real property or business entities;
        - managing of client money, securities or other assets;
        - opening or management of bank, savings or securities accounts;
        - organisations of contributions necessary for the creation, operation or management of companies;
        - creation, operation or management of trusts, companies, foundations or similar structures; or
    - by acting on behalf of and for their client in any financial or real estate transaction;

- controlled activity other than a general insurance intermediator under the Financial Services (Investment and Fiduciary Services) Act;

- dealers in high value goods whenever payment is made or received in cash and in an amount of 10,000 Euros or more;

- gambling services;

- currency exchange officers/ bureaux de change;

- money transmission/ remittance offices;

- any recognised or authorised scheme or any authorised restricted activity under the Financial Services (Collective Investment Schemes) Act 2011;

- any other financial institution (see definition in s.7(1) POCA);

- undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of DLT or similar means of recording a digital representation of an asset; and

- persons that, by way of business, exchange, or arrange or make arrangements with a view to the exchange of –
    - virtual assets for money;
    - money for virtual assets; or
    - one virtual assets for another.

1.4.4 Categories of information the GFIU can request

In exercise of its s. 1DA and 1DAA information gathering powers the GFIU may lawfully seek the following categories of information from a *relevant person*:

- information which is obtainable by a relevant person as a result of the application of their customer due diligence requirements pursuant to Part III of POCA;

- information in relation to which record keeping requirements, or reporting and disclosure requirements are imposed on a relevant person under Part III of POCA;

- any other information which is necessary to determine whether a person is a holder or beneficial owner of one or more accounts of whatever nature;

- the particulars of specified accounts, or of operations which have been carried out during a specified period; and/or

- the information is motivated by concerns relating to money laundering, an associated predicate offence, proliferation financing or terrorist financing

(section 1DB(2) POCA).

1.4.5 Criteria for GFIU information requests

Requests for further information by GFIU from persons following the submission of a report to GFIU (s.1DZ requests) do not need to be duly made in accordance with any other criteria other than that the request for such information be reasonable.

However, the requirement to comply with requests for information by the GFIU pursuant to s. IDA and IDAA only arises if such requests are duly made. Such requests are duly made if they:

- are made reasonably and in writing;

- relate to the categories of information in s.1DB(2) POCA (as discussed above);

- specify the nature of the information sought; and

- specifies a reasonable date by which, or period within which, the information must be provided

(section 1DB(1) POCA).

1.4.6 Failure to comply with S.1DA and S.1DAA GFIU requests

IT IS AN OFFENCE NOT TO COMPLY WITH A S.1DA OR S.1DAA REQUEST

A person that fails to comply with information requests duly made by the GFIU pursuant to s.1DA or s.1DDA commits an offence and shall be liable-

- on Summary convictions to a term of imprisonment up to one year, a fine up to £1,000 or both,
- on conviction on indictment to a term f imprisonment up to two years, a fine or both

(section 1DC (1) POCA).

Where such an offence is committed by a corporate body with the consent or connivance of any director, manager, secretary or other similar officer of the body corporate (or person purporting to act in such a capacity) that person will also be guilty of that offence and is liable to be proceeded against and punished accordingly (s.1DC (4) POCA).

A person charged with such an offence will have a defence if they are able to prove that the information requested by the GFIU was not within its possession; or that it was not reasonably practicable for the person to comply with the request (S.1DC(2) POCA).

1.5 GFIU requests following FIU requests – S.1G

Upon the receipt of a request from an FIU, the GFIU may use the range of its information-gathering powers available domestically to obtain information from a relevant financial business that is established in Gibraltar but operates in the territory of the requesting FIU.

1.6 Record keeping, policies and communication systems

1.6.1 Record keeping

A relevant financial business is required to maintain customer records and other information for a period of 5 years (s.25 POCA). The date on which the five-year period is deemed to commence depends on the nature of the information to be maintained. For more information on what categories of information fall within the ambit of the record-keeping requirement, and when the period of retention is deemed to commence, relevant financial businesses should refer to s.25 POCA.

1.6.2 Policies

A relevant financial business must establish and maintain appropriate and risk-sensitive reporting and record-keeping policies, controls and procedures (s.26(1) (b) and (c) POCA). These policies, controls and procedures include policies, controls and procedures which allow for full and speedy responses to requests from the GFIU, law enforcement agencies and supervisory authorities other bodies regarding:

- whether the relevant financial business maintains or has maintained a business relationship with a specified person in the five years prior to the request; or
- the information and records the relevant financial business is required to maintain pursuant to section 25 POCA;

(s. 26 (2) (e) POCA).

1.6.3 Communication systems

A relevant financial business must have systems in place which allow for full and speedy responses to a request from the GFIU, a law enforcement agency or a supervisory authority in relation to whether the relevant financial business maintains or has maintained a business relationship with a specified person in the five years prior to the request (s.30B (1) POCA). These systems must be secure channels of communication that ensure full confidentiality of the enquiries (s.30B (2) POCA).

Who are supervisory authorities?

The following bodies are supervisory authorities:

(a) the Financial Services Commission;

(b) the Authority appointed under section 2(1) of the Financial Services (Investment and Fiduciary Services) Act;

(c) the Commissioner of Banking and the Banking Supervisor;

(d) the Commissioner of Insurance and the Insurance Supervisor;

(e) the Financial Secretary, or such other person or entity as may from time to time be designated by the Minister for Finance by notice in the Gazette in respect of relevant financial businesses to which section 9(1) (POCA) applies and which are not supervised by a body listed in paragraphs (a) to (d) and (f) to (h).

(f) the Gambling Commissioner as defined in section 2 of the Gambling Act 2005;

(g) the Office of Fair Trading as defined in section 3 of the Fair Trading Act 2015 (in relation to businesses engaging in relevant financial business in accordance with sections 9(1)(h) (estate agents and letting agents), 9(1)(i) (art market participants) and 9(1)(m) (dealers in high-value goods) of POCA);

(ga) HM Customs (in relation to businesses engaging in relevant financial business in accordance with section 9(1)(j) (art storage freeport operators) of POCA)

(h) the Registrar of the Supreme Court;

(s.29 and schedule 2 part 1 POCA).

2 GFIU requests pursuant to the Register of Ultimate Beneficial Owners, Nominators and Appointors Regulations 2017

2.1 Introduction - Register of Ultimate Beneficial Owners, Nominators and Appointors Regulations 2017

The Register of Ultimate Beneficial Owners, Nominators and Appointors Regulations 2017 (the UBO regulations) are a subsidiary piece of legislation made pursuant to powers conferred upon the Government by section 184 of the Proceeds of Crimes Act for the purpose of transposing parts of the Fourth Money Laundering Directive ((EU)

2015/849) as amended by the Fifth Money Laundering Directive ((EU) 2018/843) into domestic law.

The UBO regulations provide the GFIU with information gathering powers in respect of trust information.

2.2 Requests to Trustees

Regulation 41A of the UBO regulations empowers the GFIU to make requests for trust information relating to the beneficial ownership of Gibraltar trusts that trustees are required to obtain and hold pursuant to section 61 of the Trustees Act 189 (which includes express trusts governed by Gibraltar law which do not generate tax consequences).

Trust information that the GFIU may request pursuant to this regulation includes information about the:

- trust settlor,
- trustees,
- protectors, and
- beneficiaries or class of beneficiaries and other natural persons exercising effective control over the trust.

See section 61(2) of the Trustees Act 1895 for the additional information that trustees that engage the services of a service provider where the provision of those services constitutes a relevant financial business for the purposes of section 9(1) of POCA (see [x] above for definition of a relevant financial business), or the equivalent in another jurisdiction, must obtain and hold.

GFIU requests for information under r41A of the UBO regulations must be complied with by trustees within 10 working days of receipt of such request (S61A of the Trustees Act 1895). A trustee who fails to comply with a GFIU information request within this time limit commits an offence and is liable:

- on summary conviction to a fine of up to £10,000; or

- on conviction on indictment, to imprisonment for up to two years, to a fine or to both

(s. 63 of the Trustees Act 1895).

PART 2 Information requests by law enforcement agencies and other bodies

In addition to the GFIU's information gathering powers, firms may also be required to provide customer information held to the police and or customs agencies to aid their investigations into suspected money laundering and other offences (as well as other bodies in some circumstances).

3.1 Introduction - The Proceeds of Crime Act 2015 – Part VI

Part VI of the Proceeds of Crime Act empowers non GFIU law enforcement and agencies and other bodies to collect financial information held by firms to aid investigations into suspected money laundering. For the purposes of Part VI, a money laundering investigation is an investigation into whether a person has committed a money laundering offence (section 146(5) POCA).

The investigatory powers available under Part VI which are available in money laundering investigations are:	
Section 149	Production orders;
Section 161	Disclosure orders;
Section 167	Customer information orders; and
Section 174	Account monitoring orders

(collectively "Part VI Powers" and each a "Part VI Power").

3.2 Who can exercise Part VI Powers?

The Part VI Powers are exercisable by *appropriate persons* which for the purposes of Part VI means:

- the Attorney General for the purposes of a civil recovery investigation; or
- a police officer or customs officer for the purposes of a detained cash investigation, a confiscation investigation or a money laundering investigation

(section 146(6) POCA).

The respective sections of each Part VI Power sets out what type of investigation they are exercisable in, and the relevant legal test for their operation.

Of the Part VI Powers **Customer Information Orders** and **Account Monitoring Orders** are specifically intended to facilitate *appropriate persons* in obtaining the financial information of the subjects of their investigations by allowing them to obtain the client information held by firms for the purposes of their investigations into suspected criminal conduct.

3.3 Customer Information Orders

3.3.1 What is a customer information order?

A *customer information order* is a court order issued by a judge which compels a *financial institution* identified in the order to provide any customer information that it holds relating to a particular individual with whom it has a business relationship on being required to do so by notice in writing (section 176 (6) POCA). Notice in writing may be given by electronic means (s.183(8) POCA).

Customer information orders are available to law enforcement agencies to aid in a number of investigations including a money laundering investigation and are most commonly used to determine if an unidentified account exists.

In order to obtain customer information orders an application needs to be made to the Court. These applications may be made *ex parte* to a judge in chambers (section 173 (1)

POCA) which means that the *financial institution* it is exercisable against doesn't require prior notice of the application and is likely to only hear about its obligations to provide the client information once the order has been granted and is served on the institution.

3.3.2 Who can obtain a customer information order?

A *customer information order* may be obtained by an *appropriate person* (section 167(1) POCA) and so is available to:

- the Attorney General, if the information sought is required for the purposes of a civil recovery investigation; and
- a police officer or customs officer, if the information sought is required for the purposes of a confiscation investigation or a money laundering investigation.

3.3.3 Who can a customer information order be exercised against?

Customer Information orders can be exercised against *financial institutions*. For the purposes of customer information orders *financial institutions* are persons *carrying on business in the regulated sector* (section183(4) POCA) and includes persons who have ceased to *carry on business in the regulated sector*.

Persons who have ceased carrying on business in the regulated sector can be required by a customer information orders to provide information that relates to a time when the person was carrying on business in the regulated sector and was therefore a *financial institution* (section183(5) POCA).

3.3.4 Meaning of customer information

Customer information in relation to a person and a financial institution is information whether that person holds, or has held, solely or jointly, an account or accounts or any safe deposit box at the financial institution and if so, includes the disclosure of a number of further details depending on the nature of the person involved.

Individuals

If the person is an individual *customer information* which a *financial institution* may be required to disclose includes:

- The account number or numbers (or the number or numbers of any safe deposit box);
- The individual's full name, date of birth, and most recent address and any previous addresses, and, if held jointly with another, the name; date of birth and most recent address and any previous addresses of any person who holds or has held such an account with him;
- *Accounts*: The date on which the individual began to hold an account or accounts and, if he has ceased to hold the account or accounts then the date on which he did so; or
- *Safe deposit boxes*: The date on which the box was made available to the individual, and if it has ceased to be available to him, the date on which it so ceased;
- Any evidence relation to the individual's identity that the financial institution obtained for the purposes of any legislation relation to money laundering; and
- The account number of any other accounts held at the financial institution to which the individual is a signatory including details of the person holding such other accounts.

Corporate bodies

In the case that a person is a company, limited liability partnership, or a similar body incorporated or otherwise established outside Gibraltar *customer information* that a financial institution may be required to disclose includes:

- the account number or numbers or the number of any safe deposit box;
- the person's full name;
- a description of any business which the person carries on;
- the country or territory in which it is incorporated or otherwise established and any number allocated to it by virtue of section 15 of the Companies Act 2014 or corresponding legislation of any country or territory outside Gibraltar;
- any number assigned to it for the purposes of income or other tax;
- its registered office, and any previous registered offices by virtue of the Companies Act 2014 (or corresponding earlier legislation) or anything similar under corresponding legislation of any country or territory outside Gibraltar;

- its registered office, and any previous registered offices, under the Limited Liability Partnerships Act 2008 or anything similar under corresponding legislation of any country or territory;
- *Accounts*: the date or dates on which it began to hold the account or accounts and, if it has ceased to hold the account or any of the accounts, the date or dates on which it did so; or
- *Safe deposit boxes*: the date on which the box was made available to it and if the box has ceased to be available to it the date on which it so ceased;
- Any evidence of its identity as was obtained by the financial institution under or for the purposes of any legislation relating to money laundering; and
- the full name, date of birth and most recent address and any previous addresses of any person who is a signatory to the account or any of the accounts.

3.3.5 Failure to comply with a customer information order

IT IS AN OFFENCE NOT TO COMPLY WITH A CUSTOMER INFORMATION ORDER

A *customer information order* has effect in spite of any restriction on the disclosure of information (however imposed) (s.172 POCA). A *financial institution* which is required to provide information under a *customer information order* must provide the information to the *appropriate person* in such manner, and at or by such time, as the *appropriate person* requires (s.167(7) POCA).

If a *customer information order* is properly executed and a *financial institution* fails, without a reasonable excuse, to comply with a requirement imposed on it, the *financial institution* commits a criminal offence (s. 170 POCA).

If convicted of such an offence on summary conviction a *financial institution* is liable to a fine of up to £10,000.

In addition, it is also an offence if, when complying with a customer information order, a *financial institution*:

- makes a statement which it knows to be false or misleading in a material particular, or
- recklessly makes a statement which is false or misleading in a material particular

Financial institutions who are guilty of such an offence and are liable:

- on summary conviction, to a fine not exceeding £10,000;
- on conviction on indictment, to imprisonment for a term not exceeding 2 years, to a fine or to both

(section 170(3) (4) POCA).

3.4 Account Monitoring Orders

3.4.1 What is an account monitoring order?

An *account monitoring order* is an order that a *financial institution* specified in the application for the order must, for the period stated in the order, provide account information of the description specified in the order to an *appropriate officer* in the manner, and at or by the time or times, stated in the order (s.174(7) POCA). These have effect as orders of the court (s.178(4) POCA) and have effect in spite of any restriction on the disclosure of information (however imposed) (s.177 POCA).

The duration of an account monitoring order must not exceed the period of 90 days beginning on the day that the order was made.

3.4.2 What is an account information?

Account information is information relating to an account or accounts held (whether held solely or jointly with another) at a financial institution by the person specified in the application (s.174(5) POCA).

3.4.3 Who can obtain an account monitoring order?

An *account monitoring order* may be obtained by a police or customs officer.

3.4.3 Who can a customer information order by exercised against?

Like *customer Information orders*, *account monitoring orders* can be exercised against *financial institutions* i.e. persons carrying on business in the regulated sector (section183(4) POCA).

A *financial institution* which is required to provide information under a *customer information order* must provide the information to the *appropriate person* in such manner, and at or by such time, as the *appropriate person* requires (s.167(7) POCA).

If a *customer information order* is properly executed and a *financial institution* fails, without a reasonable excuse, to comply with a requirement imposed on it, the *financial institution* commits a criminal offence (section 170 POCA). If convicted of such an offence on summary conviction a *financial institution* is liable to a fine of up to £10,000.

3.5 Production Orders

3.5.1 What is a production order?

A *production order* is a court order issued by a judge either:

- requiring the person referred to in the application who appears to be in possession or control of material to produce it to an appropriate person for him to take away; or
- requiring that person to give an appropriate person assess to the material

within the period stated in the order (s.149(4) POCA).

The period will usually be seven days beginning on the date that the order is made unless the judge making the order considers that a different time period would in the particular circumstances be appropriate (s.149(5) POCA).

In order to obtain *production orders* an application needs to be made to the Court. These applications may be made *ex parte* to a judge in chambers (s. 155 (1) POCA) which means that the person or institution it is exercisable against doesn't require prior notice of the application. *Production orders* have effect as if they were orders of the court (s.155(7) (POCA).

Access - In addition, if required to give an *appropriate person* access to material on any premises, a judge may, on an application of an *appropriate person* specifying a premises, make an order to grant entry in relation to that premises (s.151 POCA).

3.5.2 Effect of a production order

A *production order* has effect in spite of any restriction on the disclosure of information (however imposed) (s.152(4) POCA). However, it does not require disclosure of:

- documents which would the person would be entitled to refuse to produce on grounds of legal professional privilege in proceedings privileged:
- or excluded materials (for the definition of excluded materials see s.15 of the Criminal Procedure and Evidence Act 2011)

(s.152(1) and (3) POCA).

An *appropriate person* may take copies of any material which is produced, or to which access is given in compliance with a *production order* (s152(5) POCA). Material produced may be retained for as long as it is necessary to retain it (as opposed to copies of it) in connection with the investigations for which the production order was made (s.152(6) POCA) however this period may be extended in certain circumstances.

Computer information – if the material specified in a *production order* is contained in a computer, it must be provided in a form that is visible and legible, and if the order permits an *appropriate person* to take it away, it must also be provided in such a way (s.153 POCA).

3.5.3 Who can obtain a production order?

A *production order* may be obtained by an *appropriate person* (section 149(1) POCA) and so is available to:

- the Attorney General, if the information sought is required for the purposes of a civil recovery investigation; and
- a police officer or customs officer, if the information sought is required for the purposes of a confiscation investigation or a money laundering investigation.

3.5.4 Failure to comply with a production order

If a *production order* has not been complied with, an *appropriate person* may obtain a search and seizure warrant which would allow entry and search of the premises specified and the seizure and retention of any material found there which is likely to be

of substantial value to the investigation for the purpose of which the application is made (s.156 POCA).

3.6 Disclosure Orders

3.6.1 What is a disclosure order?

A *disclosure order* is a court order issued by a judge which authorises a police or customs officer to give any person it has relevant information notice in writing requiring him to do, with respect to any matter relevant to the investigations for the purposes of which the order is sought, and or all of the following:

- answer questions, either at a specified time or at once, at a specified place;
- provide information by a specified time and in a specified manner;
- produce documents, or documents of a description, either by a specified time or at once, in a specified manner

(s.161(5) POCA).

3.6.2 Effect of a disclosure order

An application for a *disclosure order* may be made *ex parte* to a judge of the Supreme Court (S.166(1) POCA.

A *disclosure order* has effect in spite of any restriction on the disclosure of information (however imposed) (s.165(6) POCA). However, it does not require:

- a person to answer privileged questions, provide any privileged information or produce a privileged document (s. 165(1) POCA); or
- production of excluded material for the definition of excluded materials see s.15 of the Criminal Procedure and Evidence Act 2011) (s.165(5) POCA).

A police or customs officer may take copies of any material which is produced (s165(7) POCA). Documents produced may be retained for as long as it is necessary to retain them (as opposed to copies of them) in connection with the investigations for which the *disclosure order* was made (s.165(8) POCA) however this period may be extended in certain circumstances.

3.6.3 Failure to comply with a disclosure order

IT IS AN OFFENCE NOT TO COMPLY WITH A DISCLOSURE ORDER

A person who fails, without a reasonable excuse, to comply with a requirement imposed on him by a *disclosure order* commits an offence (s. 163(1) POCA).

If convicted of such an offence on summary conviction a person is liable to imprisonment for up to 6 months, a fine of £10,000, or to both (s.163(2) POCA).

In addition, it is also an offence if, when complying with a *disclosure order*, a person:

- makes a statement which he knows to be false or misleading in a material particular, or
- recklessly makes a statement which is false or misleading in a material particular

(s.163(3) POCA).

Persons guilty of such an offence are liable:

- on summary conviction, to imprisonment for up to 6 months, or to a fine not exceeding the statutory maximum, or to both; or
- on conviction on indictment, to imprisonment for a term not exceeding 2 years, to a fine or to both

(section 163(4) POCA).

3.7 Policies and secure communication systems

Policies - A relevant financial business must establish and maintain appropriate and risk-sensitive reporting and record-keeping policies, controls and procedures (s.26(1) (b) and (c) POCA). These policies, controls and procedures include policies, controls and procedures which allow for full and speedy responses to requests from the GFIU, law enforcement agencies and supervisory authorities:

- whether the relevant financial business maintains or has maintained a business relationship with a specified person in the five years prior to the request; or

- the information and records the relevant financial business is required to maintain pursuant to section 25 POCA;

(s. 26 (2) (e) POCA).

Communication systems - A relevant financial business must have systems in place which allow for full and speedy responses to a request from the GFIU, a law enforcement agency or a supervisory authority in relation to whether the relevant financial business maintains or has maintained a business relationship with a specified person in the five years prior to the request (s.30B (1) POCA). These systems must be secure channels of communication that ensure full confidentiality of the enquiries (s.30B (2) POCA). (See section 1.6 above for the definition of supervisory authority).

4. External investigations – subsidiary legislation made pursuant to POCA

4.1 Introduction – subsidiary legislation

The Proceeds of Crime Act 2015 (External investigations ancillary to a criminal investigation or proceeding) Order 2019 and the Proceeds of Crime Act 2015 (External Investigations in a Civil Context) Order 2019 are both made in exercise of the powers conferred on the Government by sections 184 and 184B of POCA. They grant the police, customs agency and the Attorney General the range of their information gathering powers pursuant to Part VI POCA to assist external investigations in both criminal and civil contexts.

The following powers are available to the police, customs agency and Attorney General under these pieces of subsidiary legislation:

- Production order (and search and seizure warrants);
- Disclosure orders;
- Customer information orders; and
- Account monitoring orders.

4.2 What is an external investigation?

An *external investigation* is an investigation by an *overseas authority* into:

- whether *property* has been obtained as a result of or in connection with criminal conduct or was, or was intended to be, the instrumentalities of criminal conduct;
- the extent to or whereabouts of *property* obtained as a result of or in connection with criminal conduct; or
- whether a money laundering offence have been committed.

Who is an overseas authority?

An *overseas authority* is an authority that has responsibility in a country or territory outside Gibraltar:

- for making a request to an authority in another country or territory (including Gibraltar) to prohibit dealing with *relevant property* (property in respect of which there are reasonable grounds to believe that it may be needed to satisfy an external order which has been or which may be made (s.184D(6) POCA);
- for carrying out an investigation into whether *property* has been obtained as a result of or in connection with criminal conduct, or
- for carrying out an investigation into whether a money laundering offence has been committed;

(s.184D((9)POCA).

What is property?

Property is all property wherever situated and includes (i) money; (ii): all forms of property, real or personal, heritable or moveable; (iii) things in action and other tangible or incorporeal property (s.184D((1) (d) POCA).

5. The Terrorism Act 2018

5.1 Introduction – the Terrorism Act 2018

The terrorist financing and proliferation financing offences created in sections 35-39 of the Terrorism Act 2018 are included in the definition of money laundering in POCA. Therefore, the Part VI Powers exercisable by the non GFIU entities for the purposes of assisting money laundering investigations (the police, customs) under POCA include investigations into these specific terrorist offences.

In addition, Part VIII of the Terrorism Act 2018 grants the police powers to gather financial information from *financial institutions* in the context of terrorist investigations relating to:

- the commission, preparation or instigation of acts of terrorism;
- an act which appears to have been done for the purposes of terrorism;
- the resources of a proscribed organisation: or
- the commission, preparation or instigation of an offence under the Terrorism Act 2018 (save for the offences of encouragement of terrorism (section 12 Terrorism Act 2018) and Dissemination of terrorist publications (section 13 Terrorism Act 2018) which are excluded);

(section 3(1) Terrorism Act 2018).

The Terrorism Act 2018 provides two information gathering powers to assist terrorist investigations:

- Financial Information Orders (s.80 Terrorism Act 2018); and
- Account Monitoring Orders (s.81 Terrorism Act 2018).

5.2 Who are financial institutions?

The Terrorism Act 2018 defines *financial institutions* as:

- having the meaning attributed to financial institutions in section 7(1) of POCA; and
- including the meaning attributed to "relevant financial business" in section 9(1) of POCA; and to "credit institution" in section 7() of POCA

(para. 5(1) Schedule 7 Terrorism Act 2018).

For the purposes of *financial information orders* and *account monitoring orders* under the Terrorism Act 2018 institutions which have ceased to be *financial institutions* shall continue to be treated as so for the purposes of orders which relate to a time when the institution was a *financial institution* (para. 5(4) Schedule 7 and para. 1(5) Schedule 8 Terrorism Act 2018).

5.3 Financial Information Orders

The Terrorism Act 2018 provides the police with an information-gathering power to obtain intelligence held by *financial institutions* in the context of terrorist investigations (s.80 and Schedule 7 of the Terrorism Act 2018).

A *financial information order* is a court order issued by a judge authorising a police officer named in the order to require a *financial institution* to which the order applies to provide *customer information* for the purposes a terrorist investigation (para. 1(1) Schedule 7 Terrorism Act 2018).

5.3.1 What is customer Information?

Customer information is:

- information whether a business relationship exists or existed between a financial institution and a particular person ("a customer");
- a customer's account number;
- a customer's full name;
- a customer's date of birth;
- a customer's address or former address;
- the date on which a business relationship between a financial institution and a customer begins or ends;
- any evidence of a customer's identity obtained by a financial institution in pursuance of or for the purposes of any legislation relating to money laundering; and
- the identity of a person sharing an account with a customer.

5.3.2 Who can apply for a financial information order?

A *financial information order* application can be made by police officers of at least the rank of superintendent or the Attorney General. *Financial information orders* may be made by the stipendiary magistrate in the Magistrates Court or a judge of the Supreme Court (para. 3 Schedule 7 Terrorism Act 2018).

5.3.3 Failure to comply with a financial information order

IT IS AN OFFENCE NOT TO COMPLY WITH A FINANCIAL INFORMATION ORDER

A *financial institution* which is required to provide information under a *financial information order* must provide the information to the police officer in such manner, and at or by such time, as the police officer requires notwithstanding any restriction on the disclosure of information imposes by statute or otherwise (para. 1(3) Schedule 7 Terrorism Act 2018).

It is an offence for a *financial institution* to fail to comply with a *financial information order* (para. 1(4) Schedule 7 Terrorism Act 2018). However, a *financial institution* will have a defence if it can prove:

- that the information required was not in its possession; or
- that it was not reasonably practicable for the it to comply with the requirement

(para. 1(5) schedule 7 Terrorism Act 2018).

If convicted of the offence of failure to comply with a *financial information order* a *financial institution* is liable to a fine of up to £10,000 (para. 1(6) Schedule 7 Terrorism Act 2018).

Directors, managers, secretaries (and equivalent) may be personally guilty of this offence if it is proved that it was committed with their consent or connivance, or was attributable to their neglect (para. 7(1) schedule 7 Terrorism Act 2018) and if convicted shall be liable on summary conviction to imprisonment for up to 6 months, to a fine of up to £10,000, or both (para. 7(3) schedule 7 Terrorism Act 2018).

5.4 Account Monitoring Orders

5.4.1 What is an account monitoring order?

An *account monitoring order* is a court order that the *financial institution* specified must provide information relating to an account or accounts held at a *financial institution* by a specified person (whether solely or jointly with another) of the description specified to an *appropriate officer*:

- for the period specified in the order;
- in the manner specified in the order;
- at or by the time or times specified in the order; and
- at the place or places so specified

(s.81 and para. 2(2) and (4) schedule 8 Terrorist Act 2018).

The period of account monitoring orders must not exceed 90 days from the date the order was made (para. 2(5) schedule 8 Terrorism Act 2018).

5.4.2 Who can apply for an account monitoring order?

An application for an account monitoring order can be made by an *appropriate officer*, which for the purposes of account monitoring orders, is a police officer (para. 1(5) and 2(1) schedule 8 Terrorism Act 2018). Applications for account monitoring orders are made to a stipendiary magistrate and can be made *ex parte* in chambers (para. 2(1) and 3((1) schedule 8 Terrorism Act 2018).

5.4.3 Effect of an account monitoring order

Account monitoring orders have effect as if they were orders of the Supreme Court and in spite of any restriction on the disclosure of information (however imposed) (para. 6(1) and (2) schedule 8 Terrorism Act 2018).

6. The Drug Trafficking Offences Act 1995

6.1 Introduction – the Drug Trafficking Offences Act 1995

While not specifically intended for the purpose of aiding investigations into criminal conduct transacted or attempted to be transacted through financial institutions, the Drug Trafficking Offences Act 1995 provides the police and customs information gathering powers to aid drug trafficking investigations which could theoretically be utilised to obtain financial information held by firms.

6.2 Orders to make material available

Section 60 of the Drug trafficking offences Act 1995 permits police and customs officers to apply to the Supreme Court, for the purposes of an investigation into drug trafficking,

for an order relating to particular material or material of a particular description (s.60(1) Drug trafficking offences Act 1995).

An *order to make material available* is an order that the person who appears to the court to be in possession of the material to which the application relates shall:

- produce it to a customs or police officer for him to take away; or
- give a customs of police officer access to it

within such a period as the order may specify (s.60(2) Drug trafficking offences Act 1995). The period for compliance is 7 days unless the judge considers that a different period is appropriate in the particular circumstances (s. 60(4) Drug trafficking offences Act 1995). An application for an *order to make materials available* may be made *ex parte* to a judge in chambers (s. 60(7) Drug trafficking offences Act 1995).

Access - In addition where a judge makes an *order to make material available* in relation to material on any premises, he may, on an application of a customs or police officer, order any person who appears to him to be entitled to grant entry to the premises to allow a customs or police officer to enter the premises to obtain access to the material (s60(6) Drug trafficking offences Act 1995).

6.2.1 Effect of an order to make material available

An *order to make material available* shall have effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by statute or otherwise (s. 60(10) (b) Drug trafficking offences Act 1995). However, it does not confer any right to production of, or access to, items subject to legal privilege or excluded material (s, 60(10)(a) Drug trafficking offences Act 1995) (for the definition of items subject to legal privilege and excluded materials see s.2 (5) and s. 2(7)-(9) of the Drug trafficking offences Act 1995 respectively).

Computer information – if the material to be made available is contained in a computer

- an order to make material available shall have effect as an order to produce the material in a form in which it can be taken away and in which it is visible and legible; and
- an order to make material available shall have effect as an order to give access to the material in a form in which it is visible and legible

(s. 60(9) Drug trafficking offences Act 1995).

6.2.2 Failure to comply with an order to make information available

If an *order to make information available* has not been complied with a customs or police officer may apply for a search and seizure warrant which would allow entry and search of the premises specified and the seizure and retention of any material found there, other than items subject to legal privilege and excluded material, which is likely to be of substantial value to the investigation for the purpose of which the warrant is issued (s. 61(1) and (5) Drug trafficking offences Act 1995).

6.2.3 Offence of prejudicing an investigation

Where, in relation to an investigation into drug trafficking:

- an order under section 60 has been made or has been applied for and has not been refused; or
- a warrant under section 61 has been issued,

a person is guilty of an offence if, knowing or suspecting that the investigation is taking place, he makes any disclosure which is likely to prejudice the investigation (s.65 (1) Drug trafficking offences Act 1995).

A person guilty of such an offence shall be liable:

- on summary conviction, to imprisonment for up to 6 months or to a fine of up to £10,000 or both: and
- on conviction on indictment, to imprisonment for a term of up to 5 years or to a fine, or both

(s. 65(6) Drug trafficking offences Act 1995).

6.2.4 Copies and retention

A customs or police officer may photograph or copy, or have photographed or copied, anything which he has power to seize (s.61(5) Drug trafficking offences Act 1995). Anything which has been seized by a customs or police officer or taken away by a customs or police officer under the provisions of section 60 or 61 may be retained as long as it is necessary in all the circumstances (s.63 Drug trafficking offences Act 1995).

6.3 Orders for material relevant to overseas investigations

In addition to orders to make information available to assist local drug trafficking investigations, the mutual legal assistance provisions of Part III of the Drug trafficking offences Act 1995 provide police and customs officers information gathering power exercisable in the context of international drug trafficking investigations (s.43A Drug trafficking offences Act 1995).

Again, although not drafted specifically with the provision of financial information from financial institutions in mind, this information-gathering power may be utilised by the police and customs to obtain financial information held by financial institutions where it would assist international drug trafficking investigations in certain circumstances.

7. Criminal Procedure and Evidence Act 2011

7.1 Introduction - Criminal Procedure and Evidence Act 2011

The Criminal Procedure and Evidence Act 2011 (CPEA 2011) allows the police to obtain entry and search warrants from the Magistrates Court to aid their investigations into criminal conduct (s.12 CPEA 2011). However, s.12 CPEA 2011 warrants aren't usually available to the police in investigations into money laundering, and other offences, transacted, or attempted to be transacted, through the financial system because such information is normally held confidentially and therefore excluded for the purpose of s.12 CPEA 2011 warrants. The Terrorism Act s.79 also allows applications under s.12 CPEA to be made for summary offences under the Terrorism Act which fall within definition of "terrorist investigation".

Instead, relevant financial information may be obtained by the police from financial institutions via s.13 as read with Schedule 1 of the CPEA 2011 which provides a mechanism for obtaining certain categories of information that are not available via the s.12 CPEA warrant route.

7.2 Schedule 1 – Special Procedure for access to excluded material

7.2.1 What is a special procedure for access to excluded material order?

A *special procedure for access to excluded material order* is a court order (obtained from a judge of the Supreme Court or a stipendiary magistrate of the Magistrates Court) that a person who appears to them to be in possession of the material to which the application relates must:

- produce it to a police officer for him to take away; or
- give the police officer access to it;

  not later than 7 days after the date of the order or the end of any longer period the order specifies (para.4 schedule 1 CPEA 2011).

Material stored in any electronic form – if the material to be made available consists of information stored in any electronic form:

- a *special procedure for access to excluded material order* shall have effect as an order to produce the material in a form:
  (i) in which it can be taken away and in which it is visible and legible; or
  (ii) from which it can readily be produced in a visible and legible form;
- a *special procedure for access to excluded material order* that must give a police officer access to the material has effect as an order to give a police officer access to the material in a form in which it is visible and legible;

(para.5 schedule 1 CPEA 2011).

7. 2.2 Conditions for obtain a special procedure for access to excluded material order

A judge of the Supreme Court or a stipendiary magistrate of the Magistrates Court must be satisfied that one of two sets of access conditions are fulfilled.

First set of access conditions - The first set of access conditions is fulfilled if –

a) there are reasonable grounds for believing that:
   (i) an indictable offence has been committed;
   (ii) there is material which consists of *special procedure material* or also included *special procedure material* and does not also *include excluded material* on the premise specified in the application, or on premises occupied or controlled by a person specified in the application;

(iii) the material is likely to be of substantial value (whether by itself or together with other material) to the investigation in connection with which the application is made; and

(iv) the material is likely to be relevant evidence;

(b) other methods of obtaining the material have:

(i) been tried without success; or

(ii) not been tried because it appeared that they were bound to fail: and

(c) it is in the public interest, having regards to:

(i) the benefit likely to accrue to the investigation if the material is obtained; and

(ii) the circumstances under which the person in possession of the material holds it,

that the material should be produced or that access to it should be given (para.2 schedule 1 CPEA 2011).

Second set of access conditions – the second set of access conditions is fulfilled if:

a) there are reasonable grounds for believing that there is material which consists of or included excluded material or special procedure material on premises specified in the application, or on premises occupied or controlled by a person specified in the application;

b) but for section 13(2) of the CPEA 2011 a search of such a premises for that material could have been authorised by the issue of a warrant to a police officer under an enactment other than Schedule 1; and

c) the issue of such a warrant would have been appropriate

(para3 schedule 1 CPEA 2011).

7.2.3 What is special procedure material?

There are two types of *special procedure material*:

1. *journalistic material* which is not *excluded material*; and
2. material in the possession of a person:

- who acquired or created it in the course of any trade, business, profession or other occupation for the purpose of any paid or unpaid office; and
- who holds subject to an expressed or implied undertaking to hold it in confidence or a restriction on disclosure or an obligation of secrecy contained in any enactment (including one which comes into force after the commencement of the Criminal Procedure and Evidence Act 2011 comes into force) unless the later enactment limits this power;

(s.18 CPEA).

7.2.4 What is journalist material which is excluded material?

Journalist material means material acquired or created for the purposes of journalism. Such material is only journalistic material if it is in the possession of a person who acquired or created it for the purposes of journalism which included a person who receives material from someone who intends that the recipient will use it for the purposes of journalism (s17 CPEA).

Journalistic material is *excluded material* if it is journalistic material which a person holds in confidence and which consists of documents (anything in or on which information of any description is recorded, and includes an electronic record of data); or records other than documents (s.15(1)(c) CPEA). All other journalistic material is special procedure material. For the definition of *excluded material* see s.15 CPEA 2011).

7.2.5 Effect of a special procedure for access to excluded material order

An application for a *special procedure for access to excluded material order* must be made *inter partes* and notice of an application for such an order must be served on the person intended to provide the material. intended disclosing entity (paras 7 and 8 schedule 1 CPEA 2011).

Once served with such a notice, a person must not, without leave of a judge or magistrate or the written permission of a police officer, conceal, destroy, alter or dispose of the material to which the application relates until:

- the application is dismissed or abandoned; or
- he has complied with the order made on application

(para11 schedule 1 CPEA).

If a person fails to comply with a *special procedure for access to excluded material order* or contravenes the Para 11 Schedule 1 CPEA 2011 obligation not to conceal, destroy, alter or dispose of material, a judge of the Supreme Court may deal with him as if he had committed a contempt of the Supreme Court and any enactment relating to contempt of the Supreme Court will have effect in relation to such a failure (para15 schedule 1 CPEA 2011).

In addition, there are circumstances in which a police officer may apply to a judge or magistrate for a warrant authorising a police officer to enter and search the premises and seize materials (paras 12 and 13 schedule 1 CPEA 2011).